Benutzerhandbuch

Allen-Bradley

GuardLogix 5570-Steuerungen

Bestellnummern 1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP, 1756-L73SXT, 1756-L7SPXT, 1756-L72EROMS

Studio 5000 Automation Engineering & Design Environment

Übersetzung der Originalanleitung

Wichtige Hinweise für den Anwender

Lesen Sie vor dem Installieren, Konfigurieren, Betreiben oder Warten des Produkts dieses Dokument sowie die im Abschnitt zu den weiteren Ressourcen aufgeführten Dokumente im Zusammenhang mit der Installation, der Konfiguration und dem Betrieb dieser Anlage. Anwender sind angehalten, sich mit den Anweisungen zur Installation und Verdrahtung sowie mit allen geltenden Richtlinien, Gesetzen und Standards vertraut zu machen.

Aktivitäten, einschließlich Installation, Anpassung, Inbetriebnahme, Verwendung, Montage, Demontage und Wartung, müssen von entsprechend geschulten Fachkräften gemäß den anwendbaren Verfahrensregeln durchgeführt werden.

Wenn dieses Gerät in einer nicht vom Hersteller angegebenen Weise verwendet wird, kann der Schutz des Geräts beeinträchtigt werden.

Unter keinen Umständen haftet Rockwell Automation, Inc. für indirekte oder Folgeschäden, die aufgrund der Verwendung oder Anwendung dieser Geräte entstehen.

Die in diesem Handbuch aufgeführten Beispiele und Abbildungen dienen ausschließlich der Veranschaulichung. Aufgrund der zahlreichen Variablen und Anforderungen, die mit einer bestimmten Installation einhergehen, übernimmt Rockwell Automation, Inc. keine Verantwortung oder Haftung für die tatsächliche Verwendung auf der Grundlage der Beispiele und Abbildungen.

Rockwell Automation, Inc. übernimmt keine Patenthaftung hinsichtlich der Verwendung der in diesem Handbuch beschriebenen Informationen, Schaltkreise, Geräte oder Software.

Die Vervielfältigung des Inhalts dieses Handbuchs, ganz oder in Auszügen, bedarf der schriftlichen Genehmigung von Rockwell Automation, Inc.

In dieser Publikation werden nach Bedarf folgende Hinweise verwendet, um Sie auf bestimmte Sicherheitsaspekte aufmerksam zu machen.

	WARNUNG: Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die in explosionsgefährdeten Umgebungen zu einer Explosion und damit zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können.
	ACHTUNG: Dieser Hinweis macht Sie auf Vorgehensweisen und Zustände aufmerksam, die zu Verletzungen oder Tod, Sachschäden oder wirtschaftlichen Verlusten führen können. Die Achtungshinweise helfen Ihnen, eine Gefahr zu erkennen, die Gefahr zu vermeiden und die Folgen abzuschätzen.
IMPORTANT	Dieser Hinweis enthält Informationen, die für den erfolgreichen Einsatz und das Verstehen des Produkts besonders wichtig sind.

Etiketten mit besonderen Sicherheitshinweisen können auch am Gerät oder im Inneren des Geräts angebracht sein.

	STROMSCHLAGGEFAHR: Solche an der Außenseite oder im Inneren des Geräts, z. B. des Antriebs oder Motors, angebrachte Etiketten weisen darauf hin, dass möglicherweise eine gefährliche Spannung anliegt.
	VERBRENNUNGSGEFAHR: Solche an der Außenseite oder im Inneren des Geräts, z. B. des Antriebs oder Motors, angebrachte Etiketten weisen darauf hin, dass Oberflächen sehr heiß werden können und eine Verbrennungsgefahr besteht.
	LICHTBOGENGEFAHR: Solche an der Außenseite oder im Inneren des Geräts, z. B. eines Motor Control Center, angebrachte Etiketten weisen darauf hin, dass die Gefahr der Bildung eines Lichtbogens besteht. Lichtbögen können schwere, lebensgefährliche Verletzungen verursachen. Tragen Sie ordnungsgemäße persönliche Schutzausrüstung (PSA). Befolgen Sie ALLE Vorschriften für sicheres Arbeiten und persönliche Schutzausrüstung (PSA).

Allen-Bradley, Armor, ControlFLASH, ControlLogix, DriveLogix, FlexLogix, Guard I/O, GuardLogix, Integrated Architecture, Kinetix, Logix5000, PanelView, PhaseManager, PLC-5, POINT Guard I/O, PowerFlex, Rockwell Automation, Rockwell Software, RSLinx, RSLogix, RSNetWorx, Studio 5000, Studio 5000 Automation Engineering & Design Environment und Studio 5000 Logix Designer sind Marken von Rockwell Automation, Inc.

ControlNet, DeviceNet und EtherNet/IP sind Marken von ODVA. Marken, die nicht Rockwell Automation gehören, sind das Eigentum der jeweiligen Unternehmen.

Dieses Handbuch enthält neue und aktualisierte Informationen.

Neue und aktualisierte Informationen

In dieser Tabelle sind die Änderungen für diese Version aufgeführt.

Thema	Seite
Abschnittstitel wurde von „Weitere Ressourcen“ auf „Weitere Informationen“ geändert.	14
Die Beschreibung der Spalte „Quelle“ wurde von „Kinetix®-Servoantriebe“ auf „Antriebe“ geändert.	14
Die Informationen zu Antrieben wurden um die Verweise auf das „Kinetix 5700 Servo Drives User Manual“ und das „PowerFlex® 527 Adjustable Frequency AC Drive User Manual“ ergänzt.	14
Informationen zu vorherigen Versionen wurden aus der Tabelle mit unterstützten Funktionen entfernt.	23
Der Spaltentitel wurde von „Version 24“ in „Version 24 und höher“ geändert.	23
Einführungssatz und Abbildung 10 wurden hinzugefügt.	52
SNN-Zuweisungsinhalte wurden der Tabelle „Wichtig“ hinzugefügt.	53
Abbildung 14 wurde überarbeitet und umfasst nun PowerFlex 527- und Kinetix 5700-Antriebe.	60
Den Adressinformationen für Antriebe wurden die Kinetix 5700- und PowerFlex 527-Antriebe hinzugefügt.	78
Der Titel von Tabelle 20 wurde überarbeitet und die Tabelleninformationen wurden um Informationen zu weiteren Antriebe ergänzt.	78
Weitere Informationen und Verweise zu den Kinetix 5700- und PowerFlex 527-Antrieben wurden hinzugefügt.	79

Notizen:

Vorwort

Informationen über GuardLogix-Steuerungen 11
Steuerungen für den Einsatz unter extremen Umgebungsbedingungen 12
Armor GuardLogix-Steuerungen 12
Studio 5000-Umgebung 12
Terminologie 13
Weitere Informationen 14

Kapitel 1

Systemüberblick

Anforderungen an Sicherheitsanwendungen 17
Sicherheitsnetzwerknummer 17
Sicherheits-Task-Signatur 18
Unterscheiden zwischen Standard- und Sicherheitskomponenten 18
HMI-Geräte 19
Datenflussfunktionen der Steuerung 19
Auswählen der Systemhardware 20
Primärsteuerung 20
Sicherheitspartner 21
Chassis 21
Netzteil 21
Auswählen von Sicherheits-E/A-Geräten 21
Auswählen von Kommunikationsnetzwerken 22
Programmieranforderungen 22

Kapitel 2

Installation der Steuerung

Vorsichtsmaßnahmen 25
Informationen über Umgebung und Gehäuse 25
Programmierbare Elektroniksysteme (PES) 26
Ziehen und Stecken unter Spannung 26
Zulassung für explosionsgefährdete Standorte – Nordamerika 26
Zulassung für explosionsgefährdete Standorte – Europa 27
Verhindern elektrostatischer Entladung 28
Sicherstellen der Verfügbarkeit aller Komponenten 28
Installieren eines Chassis und eines Netzteils 29
Einsetzen der Steuerung in das Chassis 29
Einbauen oder Ausbauen einer Speicherkarte 31
Ausbauen der SD-Karte 31
Einbauen der SD-Karte 32
Herstellen einer Kommunikationsverbindung 33
Update der Steuerung 36
Verwenden der Software ControlFLASH zum Aktualisieren der Firmware 36
Verwenden von AutoFlash zum Aktualisieren der Firmware 37
Auswählen der Betriebsart der Steuerung 38
Ändern der Betriebsart über den Schlüsselschalter 38
Ändern der Betriebsart über die Anwendung Logix Designer 39
Deinstallieren eines Energiespeichermoduls (ESM) 39
Installieren eines Energiespeichermoduls (ESM) 41

Kapitel 3

Konfiguration der Steuerung

Erstellen eines Steuerungsprojekts 43
Elektronische Codierung 46
Weitere Informationen 46
Festlegen von Kennwörtern für die Sicherheitssperrung- und -entsperrung. 47
Schützen der Sicherheits-Task-Signatur im Run-Modus 47
Austausch eines E/A-Geräts 48
Aktivieren der Zeitsynchronisierung. 49
Konfigurieren einer Peer-Sicherheitssteuerung 50

Kapitel 4

Kommunikation über Netzwerke

Das Sicherheitsnetzwerk. 51
Verwalten der Sicherheitsnetzwerknummer 51
Zuordnen der Sicherheitsnetzwerknummer (SNN) 53
Ändern der Sicherheitsnetzwerknummer (SNN). 54
EtherNet/IP-Kommunikation 57
Produzieren und Konsumieren von Daten über ein EtherNet/IP-Netzwerk 58
Verbindungen über das EtherNet/IP-Netzwerk. 58
Beispiele für die EtherNet/IP-Kommunikation 59
EtherNet/IP-Verbindungen für Sicherheits-E/A-Geräte. 60
EtherNet/IP-Standardverbindungen. 61
ControlNet-Kommunikation. 62
Produzieren und Konsumieren von Daten über ein ControlNet-Netzwerk. 62
Verbindungen über das ControlNet-Netzwerk 63
Beispiel für die ControlNet-Kommunikation. 63
ControlNet-Verbindungen für dezentrale E/A 64
DeviceNet-Kommunikation 64
DeviceNet-Verbindungen für Sicherheits-E/A-Geräte. 65
Standard-DeviceNet-Verbindungen 66

Kapitel 5

Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen

Hinzufügen von Sicherheits-E/A-Geräten 67
Konfigurieren von Sicherheits-E/A-Geräten 68
Festlegen der IP-Adresse mit Network Address Translation (NAT) 69
Festlegen der Sicherheitsnetzwerknummer (SNN). 71
Verwenden von Unicast-Verbindungen auf EtherNet/IP-Netzwerken 71
Festlegen der Reaktionszeitgrenze der Verbindung. 71
Spezifizieren des angeforderten Paketintervalls (RPI). 72
Anzeigen der beobachteten maximalen Netzwerkverzögerung. 72
Festlegen der erweiterten Parameter für die Reaktionszeitgrenze der Verbindung 73
Verstehen der Konfigurationssignatur 75
Konfiguration über die Anwendung Logix Designer. 75
Anderer Konfigurationsverwalter (Listen-only-Verbindung). 76
Zurücksetzen der Verwaltungsrechte an Sicherheits-E/A-Geräten. 76

Adressieren von Sicherheits-E/A-Daten 77
Adressformat eines Sicherheits-E/A-Moduls 77
Adressformat von Kinetix 5500-, Kinetix 5700- und PowerFlex 527-Antrieben 78
Überwachen des Sicherheits-E/A-Gerätestatus 79
Zurücksetzen eines Moduls auf die Werkseinstellungen 80
Austauschen eines Geräts über die Anwendung Logix Designer 81
Austausch bei aktivierter Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits- (Task-) Signatur vorliegt) 82
Austausch bei aktivierter Option „Configure Always“ (Immer konfigurieren) 86
Austauschen eines POINT Guard I/O-Moduls über die Software RSNetWorx for DeviceNet 87

Kapitel 6

Entwicklung von Sicherheitsanwendungen

Die Sicherheits-Task 92
Spezifizieren der Sicherheits-Task-Zeitspanne 92
Ausführen der Sicherheits-Task 93
Sicherheitsprogramme 93
Sicherheitsroutinen 94
Sicherheits-Tags 94
Tag-Typ 95
Datentyp 95
Bereich 96
Klasse 97
Konstanter Wert 98
Externer Zugriff 98
Produzierte/konsumierte Sicherheits-Tags 98
Konfigurieren der Sicherheitsnetzwerknummern von Peer-Sicherheitssteuerungen 99
Erstellen eines Sicherheits-Tags 101
Konsumieren von Sicherheits-Tag-Daten 102
Zuordnen von Sicherheits-Tags 104
Einschränkungen 104
Erstellen von Tag-Zuordnungspaaren 105
Überwachen des Tag-Zuordnungsstatus 106
Schutz von Sicherheitsanwendungen 106
Sicherheitssperre der Steuerung 106
Erstellen einer Sicherheits-Task-Signatur 108
Einschränkungen bei der Programmierung 110

Kapitel 7

Schalten der Steuerung in den Online-Modus

Verbinden der Steuerung mit dem Netzwerk 111
Verbinden Ihres EtherNet/IP-Geräts mit dem Computer 111
Verbinden Ihres ControlNet-Kommunikationsmoduls oder Ihres DeviceNet-Scanners mit Ihrem Computer 112
Konfigurieren eines EtherNet/IP-, ControlNet- oder DeviceNet-Treibers 112
Faktoren, die das Schalten in den Online-Modus beeinflussen 112
Übereinstimmung zwischen Projekt und Steuerung 113

Firmware-Versionsübereinstimmung 113
Sicherheitsstatus/-fehler 113
Sicherheits-Task-Signatur sowie sicherheitsgesperrter und-entsperrter Zustand 114
Herunterladen 115
Hochladen 116
Schalten in den Online-Modus 117

Kapitel 8

Speichern und Laden von Projekten mithilfe des nichtflüchtigen Speichers

Verwenden von Speicherkarten für nichtflüchtigen Speicher 119
Speichern eines Sicherheitsprojekts 120
Laden eines Sicherheitsprojekts 121
Verwenden von Energiespeichermodulen 122
Speichern des Programms im integrierten, nichtflüchtigen Speicher 122
Löschen des Programms aus dem integrierten nichtflüchtigen Speicher 123
Abschätzen der ESM-Unterstützung für die Uhrzeit 124
Verwalten der Firmware mit Firmware Supervisor 124

Kapitel 9

Zustandsüberwachung und Fehlerbehebung

Anzeige des Status über die Online-Leiste 125
Überwachen der Verbindungen 126
Alle Verbindungen 126
Sicherheitsverbindungen 127
Überwachen von Status-Flags 127
Überwachen des Sicherheitsstatus 128
Steuerungsfehler 128
Nicht korrigierbare Steuerungsfehler 129
Nicht korrigierbare Sicherheitsfehler in der Sicherheitsanwendung 129
Korrigierbare Sicherheitsfehler in der Sicherheitsanwendung 129
Anzeigen von Fehlern 130
Fehlercodes 130
Entwickeln einer Fehlerroutine 131
Programmfehlerroutine 131
Steuerungsfehlerbehebungsprogramm 131
Verwendung der GSV/SSV-Befehle 132

Anhang A

Statusanzeigen

Statusanzeigen der Steuerung 135
Statusanzeige der Steuerung 136
Sicherheitsbezogene Statusmeldungen 136
Allgemeine Statusmeldungen 137
Fehlermeldungen 138
Meldungen zu schwerwiegenden, korrigierbaren Fehlern 139
E/A-Fehlercodes 140

Anhang B

Wechsel des Steuerungstyps

Wechsel von Standard- zu Sicherheitssteuerung 143
Wechsel von Sicherheits- zu Standardsteuerung 144
Wechsel von Sicherheitssteuerungstypen..... 144
Weitere Informationen..... 145

Notizen:

Thema	Seite
Informationen über GuardLogix-Steuerungen	11
Studio 5000-Umgebung	12
Terminologie	13
Weitere Informationen	14

Dieses Handbuch ist eine Anleitung zur Verwendung von GuardLogix® 5570-Steuerungen in einer Studio 5000 Logix Designer™-Anwendung. Es enthält eine Beschreibung der GuardLogix-spezifischen Verfahren, die zum Konfigurieren und Bedienen der Steuerung sowie zur Fehlerbehebung eingesetzt werden.

Das Handbuch richtet sich an Personen, die für die Konzeption, Installation, Programmierung und Wartung von Steuerungssystemen, die GuardLogix-Steuerungen der Serie 5570 einsetzen, verantwortlich sind.

Grundlegende Kenntnisse im Umgang mit elektrischen Schaltungen und Relaislogik werden vorausgesetzt. Weitere Anforderungen sind eine Ausbildung sowie Erfahrung in Erstellung, Betrieb und Wartung von Sicherheitssystemen.

Ausführliche Informationen zu weiterführenden Themen über Ihre GuardLogix-Steuerung, zu den Safety Integrity Level (SIL) 3 und Performance Level (e) (SIL 3/PLe)-Anforderungen oder Informationen zu Logix-Standardkomponenten finden Sie in der Liste unter Weitere Informationen auf Seite 14.

Informationen über GuardLogix-Steuerungen

Es stehen zwei Produktreihen von GuardLogix-Steuerungen der Serie 1756 zur Verfügung. Diese Steuerungen weisen viele ähnliche Leistungsmerkmale auf, unterscheiden sich jedoch auch in einigen Eigenschaften. In Tabelle 1 sind die Unterschiede kurz zusammengefasst.

Tabelle 1 – Unterschiede zwischen der Steuerung GuardLogix 5570 und GuardLogix 5560

Funktion	**GuardLogix 5570-Steuerungen** (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	**GuardLogix 5560-Steuerungen** (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Unterstützung einer Uhr und Backup zur Absicherung des Speichers beim Herunterfahren	Energiespeichermodul (ESM)	Batterie
Kommunikationsanschlüsse (integriert)	USB	seriell
Anschlüsse, Steuerung	500	250
Speicherung, nichtflüchtig	SD-Karte	CompactFlash (CF)-Karte
Statusanzeigen/-leuchten	Bildlauf-Statusanzeige und Statusanzeigen	Statusanzeigen/-leuchten
Programmierwerkzeug	Studio 5000-Umgebung, Version 21 oder höher Software RSLogix™ 5000, Version 20 oder höher	Software RSLogix 5000, Version 14 Software RSLogix 5000, Version 16 oder höher

Tabelle 1 – Unterschiede zwischen der Steuerung GuardLogix 5570 und GuardLogix 5560

Funktion	GuardLogix 5570-Steuerungen (1756-L71S, 1756-L72S, 1756-L73S, 1756-L7SP 1756-L73SXT, 1756-L7SPXT)	GuardLogix 5560-Steuerungen (1756-L61S, 1756-L62S, 1756-L63S, 1756-LSP)
Benutzerhandbuch	• Studio 5000-Umgebung: dieses Handbuch • Software RSLogix 5000: 1756-UM020	1756-UM020
Sicherheitsreferenzhandbuch	• Studio 5000-Umgebung: 1756-RM099 • Software RSLogix 5000: 1756-RM093	1756-RM093

Steuerungen für den Einsatz unter extremen Umgebungsbedingungen

Die GuardLogix-Steuerungen für extreme Umgebungsbedingungen, Bestellnummer 1756-L73SXT und 1756-L7SPXT, bieten dieselbe Funktionalität wie die Steuerung 1756-L73S, sind jedoch zusätzlich für Temperaturen von -25 bis +70 °C ausgelegt).

WICHTIG Logix-XT-Systemkomponenten sind nur für den Betrieb unter extremen Umgebungsbedingungen ausgelegt, wenn sie ordnungsgemäß mit anderen Logix-XT-Systemkomponenten eingesetzt werden. Bei Verwendung von Logix-XT-Komponenten mit herkömmlichen Logix-Systemkomponenten gelten die Nennwerte für extreme Umgebungen nicht mehr.

Armor GuardLogix-Steuerungen

Die Armor™ GuardLogix-Steuerung (Bestellnummer 1756-L72EROMS) kombiniert eine GuardLogix-Steuerung 1756-L72S und einen Sicherheitspartner mit zwei EtherNet/IP™-, DLR-kompatiblen Kommunikationskanälen in einem IP67-Gehäuse für die Montage auf einer Maschine. Weitere Informationen über die Armor GuardLogix-Steuerung finden Sie in der Installationsanleitung für die Armor GuardLogix-Steuerung, Publikation 1756-IN060.

Studio 5000-Umgebung

Studio 5000 Automation Engineering & Design Environment™ kombiniert Engineering- und Design-Elemente in einer gemeinsamen Umgebung. Das erste Element ist die Studio 5000-Anwendung Logix Designer. Der Logix Designer ist der neue Markenname der Software RSLogix 5000 und wird in Zukunft das Produkt sein, mit dem Logix5000™-Steuerungen für Ablauf-, Prozess-, Chargen-, Achssteuerungs-, Sicherheits- und antriebsbasierte Lösungen programmiert werden.

Die Software Studio 5000 bildet die Grundlage für alle zukünftigen Konstruktionswerkzeuge und -optionen von Rockwell Automation®. In der Studio 5000-Umgebung werden Konstrukteure alle Elemente ihres Steuerungssystems entwickeln.

Terminologie

In der folgenden Tabelle werden die in diesem Handbuch verwendeten Begriffe definiert.

Tabelle 2 – Begriffe und Definitionen

Abkürzung	Vollständiger Begriff	Definition
1oo2	One Out of Two/Einer von zweien	Bezieht sich auf die Arbeitsweise eines Multiprozessor-Sicherheitsystems.
CIP	Common Industrial Protocol	Ein Kommunikationsprotokoll, das für industrielle Automatisierungsanwendungen konzipiert ist.
CIP Safety	Common Industrial Protocol – Sicherheitszertifizierung	SIL 3/PLe-Versionen von CIP.
DC	Diagnostic Coverage/Diagnoseabdeckung	Das Verhältnis zwischen erkannter Ausfallrate und Gesamtausfallrate.
EN	Europäische Norm	Die offizielle europäische Industrienorm.
ESM	Energiespeichermodul	Dient zur Unterstützung einer Uhr und zur Absicherung des Speichers beim Herunterfahren von GuardLogix-Steuerungen der Serie 5570.
GSV	Get System Value/Systemwert abrufen	Ein Befehl, mit dem spezifizierte Steuerungsstatusinformationen abgerufen und in einem Ziel-Tag abgelegt werden.
—	Multicast	Die Übermittlung von Informationen von einem Sender zu mehreren Empfängern.
NAT	Network Address Translation	Die Übersetzung einer IP (Internet Protocol)-Adresse in eine andere IP-Adresse in einem anderen Netzwerk.
PFD	Probability of Failure on Demand/Ausfallwahrscheinlichkeit bei Anforderung	Die mittlere Wahrscheinlichkeit, dass ein System seine vorgegebene Funktion bei Anforderung nicht ausführt.
PFH	Probability of Failure per Hour/Ausfallwahrscheinlichkeit pro Stunde	Die Wahrscheinlichkeit eines gefahrbringenden Ausfalls in einem System pro Stunde.
PL	Performance Level (Leistungsstufe)	ISO 13849-1 (Sicherheitsklassifizierung).
RPI	Requested Packet Interval/angefordertes Paketintervall	Die erwartete Zeitspanne für die Produktion der Daten beim Kommunizieren über ein Netzwerk.
SNN	Sicherheitsnetzwerknummer	Eine eindeutige Nummer, die einen Abschnitt eines Sicherheitsnetzwerks identifiziert.
SSV	Set System Value/Systemwert einstellen	Ein Befehl zur Konfiguration von Steuerungssystemdaten.
—	Standard	Objekte, Tasks, Tags, Programme oder Komponenten in Ihrem Projekt, die nicht sicherheitsrelevant sind.
—	Unicast	Die Übermittlung von Informationen von einem Sender zu einem Empfänger.

Weitere Informationen

Die folgenden Dokumente enthalten weitere Informationen zu verwandten Produkten von Rockwell Automation.

Tabelle 3 – Publikationen zu GuardLogix-Steuerungen und -Systemen

Quelle		Beschreibung
Sicherheits-Anwendungsanforderungen	Steuerungssysteme GuardLogix 5570 – Sicherheitsreferenzhandbuch, Publikation 1756-RM099	Ausführliche Anforderungen zum Erreichen und Erhalten von SIL 3/PLe mit dem GuardLogix-Steuerungssystem 5570 unter Verwendung der Studio 5000-Anwendung Logix Designer.
	GuardLogix Controller Systems Safety Reference Manual, Publikation 1756-RM093	Ausführliche Anforderungen zum Erreichen und Erhalten von SIL 3/PLe mit dem GuardLogix-Steuerungssystem 5560 oder 5570 unter Verwendung der Software RSLogix 5000.
CIP Sync (Zeitsynchronisation)	Integrated Architecture® and CIP Sync Configuration Application Technique, Publikation IA-AT003	Ausführliche Informationen zur Anwendung von CIP Sync-Technologie zur Synchronisation von Uhren in einem Logix-Steuerungssystem.
Guard I/O™-Module	Guard I/O DeviceNet-Sicherheitsmodule – Benutzerhandbuch, Publikation 1791DS-UM001	Informationen zur Verwendung von Guard I/O DeviceNet-Sicherheitsmodulen.
	Guard I/O EtherNet/IP Safety Modules User Manual, Publikation 1791ES-UM001	Informationen zur Verwendung von Guard I/O EtherNet/IP-Sicherheitsmodulen.
	POINT Guard I/O™-Sicherheitsmodule – Installations- und Benutzerhandbuch, Publikation 1734-UM013	Informationen zur Installation, Konfiguration und Verwendung von POINT Guard I/O-Modulen.
	Armor GuardLogix-Steuerung – Installationsanleitung, Publikation 1756-IN060	Bietet Informationen zum Installieren und Verwenden von Armor Compact GuardLogix-Steuerungen.
Antriebe	Kinetix 5500-Servoantriebe – Benutzerhandbuch, Publikation 2198-UM001	Bietet Informationen zur Installation, Konfiguration, zum Starten und zur Fehlerbehebung Ihres Kinetix 5500-Servoantriebssystems. Enthält auch Anforderungen für die Verwendung von Kinetix 5500-Antrieben in Sicherheitsanwendungen.
	Kinetix 5700 Servo Drives User Manual, Publikation 2198-UM002	Bietet Informationen zur Installation, Konfiguration, zum Starten und zur Fehlerbehebung Ihres Kinetix 5700-Servoantriebssystems. Enthält auch Anforderungen für die Verwendung von Kinetix 5700-Antrieben in Sicherheitsanwendungen.
	PowerFlex 527 Adjustable Frequency AC Drive User Manual, Publikation 520-UM002	Bietet Informationen zur Installation, zum Starten und zur Fehlerbehebung der PowerFlex 527-Frequenzumrichter.
Hardware-Installation	ControlLogix®-Chassis und -Netzteil – Installationsanleitung, Publikation 1756-IN005	Informationen zur Installation und Erdung von ControlLogix-Chassis und -Netzteilen.
	„Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen“, Publikation 1770-4.1	Detaillierte Informationen zum Erden und Verdrahten speicherprogrammierbarer Steuerungen.
Befehle (Programmierung)	GuardLogix Safety Application Instruction Set Reference Manual, Publikation 1756-RM095	Informationen zum Befehlssatz für GuardLogix-Sicherheitsanwendungen.
	Logix5000-Steuerungen – Allgemeine Befehle – Referenzhandbuch, Publikation 1756-RM003	Bietet Programmierern detaillierte Informationen zu jedem für eine Logix5000-Steuerung verfügbaren Befehl.
	Logix5000 Controllers Motion Instructions Reference Manual, Publikation MOTION-RM002	Bietet Programmierern detaillierte Informationen zu den für eine Logix5000-Steuerung verfügbaren Achssteuerungsbefehlen.
Achssteuerung	Sercos Motion Configuration and Startup User Manual, Publikation MOTION-UM001	Einzelheiten zum Konfigurieren eines Anwendungssystems mit Sercos-Achssteuerung.
	Motion Coordinated Systems User Manual, Publikation MOTION-UM002	Einzelheiten zum Erstellen und Konfigurieren eines Anwendungssystems zur koordinierten Achssteuerung.
	Integrated Motion on the EtherNet/IP Network Configuration and Startup User Manual, Publikation MOTION-UM003	Einzelheiten zum Konfigurieren eines Anwendungssystems mit Integrated Motion über EtherNet/IP-Netzwerke.
	Integrated Motion on the EtherNet/IP Network Reference Manual, Publikation MOTION-RM003	Ausführliche Informationen zu Achssteuerungsbetriebsarten und -attributen für Integrated Motion über EtherNet/IP-Netzwerke.
Netzwerke (ControlNet™, DeviceNet, EtherNet/IP)	EtherNet/IP- Module in Logix5000- Steuerungssystemen – Benutzerhandbuch, Publikation ENET-UM001	Informationen zur Konfiguration und Verwendung von EtherNet/IP-Modulen in einem Logix5000-Steuerungssystem.
	ControlNet Modules in Logix5000 Control Systems User Manual, Publikation CNET-UM001	Informationen zur Konfiguration und Verwendung von ControlNet-Modulen in einem Logix5000-Steuerungssystem.
	DeviceNet Modules in Logix5000 Control Systems, Publikation DNET-UM004	Informationen zur Konfiguration und Verwendung von DeviceNet-Modulen in einem Logix5000-Steuerungssystem.

Tabelle 3 – Publikationen zu GuardLogix-Steuerungen und -Systemen (Fortsetzung)

Quelle		Beschreibung
PhaseManager™	PhaseManager User Manual, Publikation LOGIX-UM001	Schrittweise Anleitungen und Beispiele zur Konfiguration und Programmierung einer Logix5000-Steuerung zur Verwendung von Gerätephasen.
Programmieraufgaben und -verfahren	Logix5000 Controllers Common Procedures Programming Manual, Publikation 1756-PM001	Ermöglicht den Zugriff auf die Programmierhandbücher der Logix5000-Steuerungen, in denen Sie Informationen zum Verwalten von Projektdateien, zum Organisieren von Tags, zur Logikprogrammierung, zum Testen von Routinen, zur Fehlerbehandlung und mehr finden.
	Logix5000 Controllers Execution Time and Memory Use Reference Manual, Publikation 1756-RM087	Unterstützung beim Abschätzen der Speicherbelegung und der Ausführungszeit programmierter Logik sowie bei der Auswahl der verschiedenen Programmieroptionen.

Die Publikationen stehen unter http://www.rockwellautomation.com/literature zur Ansicht oder zum Download bereit. Wenn Sie eine gedruckte Version der technischen Dokumentation benötigen, wenden Sie sich an den für Sie zuständigen Allen-Bradley-Distributor oder Vertriebsbeauftragten von Rockwell Automation.

Notizen:

Systemüberblick

Thema	Seite
Anforderungen an Sicherheitsanwendungen	17
Unterscheiden zwischen Standard- und Sicherheitskomponenten	18
Datenflussfunktionen der Steuerung	19
Auswählen der Systemhardware	20
Auswählen von Sicherheits-E/A-Geräten	21
Auswählen von Kommunikationsnetzwerken	22
Programmieranforderungen	22

Anforderungen an Sicherheitsanwendungen

Das Steuerungssystem GuardLogix 5570 ist für die Verwendung in Sicherheitsanwendungen bis zu und einschließlich Safety Integrity Level Claim Limit (SIL CL) 3 und Performance Level (e) zertifiziert, wobei der abgeschaltete Zustand der sichere Zustand ist. Die Anforderungen an Sicherheitsanwendungen umfassen die Einschätzung der Wahrscheinlichkeit von Ausfallraten, wie z. B.:

- Ausfallwahrscheinlichkeit bei Anforderung (PFD)
- Ausfallwahrscheinlichkeit pro Stunde (PFH)
- Einstellung von Systemreaktionszeiten
- Funktionsverifikationsprüfungen, die die SIL 3/PLe-Kriterien erfüllen

Für auf GuardLogix basierende SIL 3-/PLe-Sicherheitsanwendungen müssen mindestens eine Sicherheitsnetzwerknummer (SNN) und eine Sicherheits-Task-Signatur verwendet werden. Beide beeinflussen die Konfiguration von Steuerung und E/A sowie die Netzwerkkommunikation.

Weitere Informationen zu den Anforderungen an Sicherheitssysteme nach SIL 3 und PLe, einschließlich der Intervalle der funktionellen Validierungsprüfungen, der Berechnungen von Systemreaktionszeiten und Ausfallwahrscheinlichkeiten (PFD/PFH), sind der Publikation 1756-RM099, GuardLogix 5570 Controller Systems Safety Reference Manual, zu entnehmen. Sie müssen diese Anforderungen gelesen, verstanden und erfüllt haben, bevor Sie mit einem auf einer GuardLogix-Steuerung basierenden SIL 3-, PLe-Sicherheitssystem arbeiten.

Sicherheitsnetzwerknummer

Die Sicherheitsnetzwerknummer (SNN) muss eine eindeutige Nummer sein, welche die Sicherheits-Subnetze kennzeichnet. Jedes Sicherheits-Subnetz, das die Steuerung für die Sicherheitskommunikation verwendet, muss über eine eindeutige SNN verfügen. Jedes Sicherheits-E/A-Gerät muss auch mit der SNN des Sicherheits-Subnetzes konfiguriert werden. Die SNN kann automatisch oder manuell zugeordnet werden.

Informationen zum Festlegen der SNN finden Sie unter Verwalten der Sicherheitsnetzwerknummer auf Seite 51.

Sicherheits-Task-Signatur

Die Sicherheits-Task-Signatur besteht aus einer Identifikationsnummer (ID-Nummer), Datum und Zeit, die in eindeutiger Weise den Sicherheitsteil eines Projekts kennzeichnen. Dies beinhaltet die Sicherheitslogik, die Daten sowie die Konfiguration. Das GuardLogix-System verwendet die Sicherheits-Task-Signatur, um die Integrität des Projekts festzulegen und Ihnen die Möglichkeit zur Prüfung zu geben, ob das richtige Projekt auf die Zielsteuerung heruntergeladen wird. Die Möglichkeit, die Sicherheits-Task-Signatur erstellen, aufzeichnen und prüfen zu können, ist ein obligatorischer Bestandteil des Entwicklungsprozesses einer Sicherheitsanwendung.

Weitere Informationen finden Sie unter
Erstellen einer Sicherheits-Task-Signatur auf Seite 108.

Unterscheiden zwischen Standard- und Sicherheitskomponenten

Steckplätze eines GuardLogix-Systemchassis, die nicht für die Sicherheitsfunktion verwendet werden, können mit anderen ControlLogix-Modulen besetzt werden, die gemäß der Niederspannungs- und der EMV-Richtlinien zertifiziert sind. Die CE-Zertifizierung für die speicherprogrammierbare Steuerung der >ControlLogix-Produktfamilie und Informationen dazu, welche Module zertifiziert sind, finden Sie unter http://www.rockwellautomation.com/rockwellautomation/certification/ce.page.

Sie müssen eine klare, logische und sichtbare Unterscheidung zwischen den Sicherheits- und Standardteilen des Steuerungsprojekts vornehmen. Um Sie beim Festlegen dieser Unterscheidung zu unterstützen, bietet die Anwendung Logix Designer Sicherheitsidentifikationssymbole, mit denen Sie die Sicherheits-Task, Sicherheitsprogramme, Sicherheitsroutinen und Sicherheitskomponenten kennzeichnen können. Darüber hinaus verwendet die Anwendung Logix Designer ein Sicherheitsklassenattribut, das immer dann sichtbar ist, wenn die Eigenschaften von Sicherheits-Tasks, Sicherheitsprogrammen, Sicherheitsroutinen, Sicherheits-Tags oder Sicherheits-Add-On-Befehlen angezeigt werden.

Die Steuerung gestattet nicht, dass Sicherheits-Tag-Daten von externen Bedienerschnittstellengeräten (HMI-Geräten) oder über Nachrichtenbefehle von Peer-Steuerungen überschrieben werden. Die Anwendung Logix Designer kann Sicherheits-Tags schreiben, wenn die GuardLogix-Steuerung sicherheitsentsperrt ist, über keine Sicherheits-Task-Signatur verfügt und keine Sicherheitsfehler aufweist.

Publikation 1756-UM001, ControlLogix-System – Benutzerhandbuch, enthält Informationen zur Verwendung von ControlLogix-Geräten in nicht sicherheitsrelevanten Standardanwendungen.

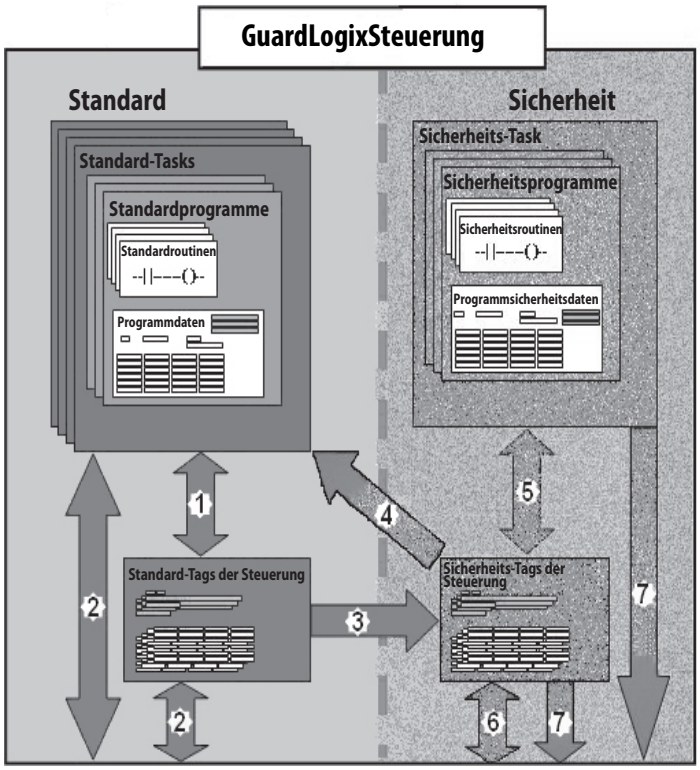
HMI-Geräte

HMI-Geräte (Bedienerschnittstellengeräte) können mit GuardLogix-Steuerungen verwendet werden. Mit HMI-Geräten kann auf Standard-Tags zugegriffen werden, wie mit einer Standardsteuerung. Sie können allerdings nicht auf Sicherheits-Tags schreiben, da diese für HMI-Geräte schreibgeschützt sind (Nur-Lese-Status).

Datenflussfunktionen der Steuerung

Diese Abbildung veranschaulicht die Flussfunktionen für Standard- und Sicherheitsdaten der GuardLogix-Steuerung.

Abbildung 1 – Datenflussfunktionen der



Nr.	Beschreibung	
1	Standard-Tags und Logik verhalten sich genau so wie in der Logix-Standardplattform.	
2	Standard-Tag-Daten, programm- sowie steuerungsbezogen, können mit externen HMI-Geräten, PCs und anderen Steuerungen ausgetauscht werden.	
3	GuardLogix-Steuerungen sind integrierte Steuerungen, die in der Lage sind, Standard-Tag-Daten in Sicherheits-Tags zu verlagern (Zuordnung), damit sie in der Sicherheits-Task verwendet werden können.	
		ACHTUNG: Diese Daten dürfen nicht verwendet werden, um einen SIL 3/PLe-Ausgang direkt zu steuern.
4	Steuerungsbezogene Sicherheits-Tags können direkt von der Standardlogik gelesen werden.	
5	Sicherheits-Tags können von der Sicherheitslogik gelesen oder geschrieben werden.	
6	Sicherheits-Tags können zwischen Sicherheitssteuerungen über Ethernet- oder ControlNet-Netzwerke ausgetauscht werden (einschließlich GuardLogix-Steuerungen der Serien 1756 und 1768).	
7	Sicherheits-Tag-Daten, programm- oder steuerungsbezogen, können von externen Geräten, wie HMI-Geräten, PCs oder anderen Standardsteuerungen, gelesen werden.	
	WICHTIG	Sobald diese Daten gelesen wurden, gelten sie als Standarddaten, nicht als SIL 3/PLe-Daten.

Auswählen der Systemhardware

Das GuardLogix-System unterstützt SIL 3- und PLe-Sicherheitsanwendungen. Die GuardLogix-Steuerung besteht aus einer Primärsteuerung und einem Sicherheitspartner, die gemeinsam in einer 1oo2-Architektur verwendet werden können. In Tabelle 4 finden Sie Bestellnummern für Primärsteuerungen und Sicherheitspartner.

Der Sicherheitspartner muss im Steckplatz unmittelbar rechts neben die Primärsteuerung installiert werden. Die Haupt- und Nebenversionen der Firmware der Primärsteuerung und des Sicherheitspartners müssen exakt übereinstimmen, damit sie eine für Sicherheitsanwendungen erforderliche Steuerungspartnerschaft aufbauen können.

Tabelle 4 – Bestellnummern für Primärsteuerung und entsprechenden Sicherheitspartner

Primärsteuerung	Sicherheitspartner
1756-L71S, 1756-L72S, 1756-L73S	1756-L7SP
1756-L73SXT	1756-L7SPXT

Primärsteuerung

Die Primärsteuerung ist der Prozessor, der Standard- und Sicherheitsfunktionen ausführt und der bei sicherheitsrelevanten Funktionen mit dem Sicherheitspartner im GuardLogix-Steuerungssystem kommuniziert. Folgende Funktionen zählen zu den Standardfunktionen:

- E/A-Steuerung
- Logik
- Zeitmessung
- Zählung
- Berichtserstellung
- Kommunikation
- Arithmetische Berechnungen
- Datendatei-Bearbeitung

Die Primärsteuerung besteht aus einem zentralen Prozessor, einer E/A-Schnittstelle und einem Speicher.

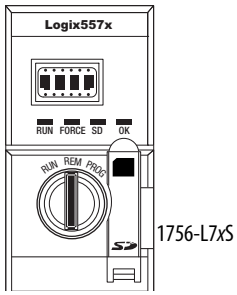
Tabelle 5 – Speicherkapazität

Best.- Nr.	Anwenderspeicher (RAM-Kapazität)	
	Standard-Tasks und -komponenten	Sicherheits-Tasks und -komponenten
1756-L71S	2 MB	1 MB
1756-L72S	4 MB	2 MB
1756-L73S,1756-L73SXT	8 MB	4 MB

Ein Drei-Positionen-Schlüsselschalter auf der Vorderseite der Primärsteuerung regelt die Betriebsmodi der Steuerung. Folgende Modi stehen zur Verfügung:

- RUN
- PROGram
- REMote – dieser softwareaktivierte Modus kann Program, Run oder Test sein

Abbildung 2 – Schlüsselschalterpositionen



Sicherheitspartner

Der Sicherheitspartner ist ein Coprozessor, der für einen isolierten zweiten Kanal (Redundanz) für sicherheitsrelevante Funktionen im System sorgt.

Der Sicherheitspartner verfügt über keinen Schlüsselschalter oder Kommunikationsanschluss. Seine Konfiguration und sein Betrieb werden durch die Primärsteuerung geregelt.

Chassis

Das ControlLogix-Chassis stellt die physische Verbindung zwischen den Modulen und der GuardLogix-Steuerung bereit.

Netzteil

Die ControlLogix-Netzteile, die auf Seite 29 aufgeführt sind, eignen sich für den Einsatz in SIL 3-Anwendungen. Für den SIL 3-Betrieb des Netzteils ist keine zusätzliche Konfiguration oder Verkabelung erforderlich.

Auswählen von Sicherheits-E/A-Geräten

Sicherheitseingangs- und -ausgangsgeräte (z. B. Sensoren und Aktoren) können an die Sicherheits-E/A in DeviceNet- oder EtherNet/IP-Netzwerken angeschlossen werden. Dieser Anschluss ermöglicht die Steuerung von Ausgangsgeräten durch ein GuardLogix-Steuerungssystem über die DeviceNet- oder EtherNet/IP-Kommunikation.

Aktuelle Informationen zu den verfügbaren Bestellnummern, zertifizierten Serien und Firmwareversionen für die Sicherheits-E/A finden Sie unter http://www.rockwellautomation.com/rockwellautomation/certification/safety.page.

Auswählen von Kommunikationsnetzwerken

Die GuardLogix-Steuerung unterstützt Kommunikation, die ihr Folgendes ermöglicht:

- Verteilen und Steuern von Sicherheits-E/A in DeviceNet- oder EtherNet/IP-Netzwerken.
- Verteilen und Steuern von dezentralen Sicherheits-E/A in DeviceNet-, EtherNet/IP- oder ControlNet-Netzwerken.
- Produzieren und Konsumieren von Sicherheits-Tag-Daten zwischen GuardLogix-Steuerungen der Serien 1756 und 1768 über Ethernet/IP- oder ControlNet-Netzwerke oder innerhalb desselben ControlLogix-Chassis.
- Verteilen und Steuern von Standard-E/A in Ethernet-, ControlNet- oder DeviceNet-Netzwerken.

Verwenden dieser Kommunikationsmodule zum Bereitstellen einer Schnittstelle zwischen GuardLogix-Steuerungen und Netzwerkgeräten.

Tabelle 6 – Kommunikationsmodule

Als Schnittstelle zwischen	Verwenden Sie dieses Modul	Siehe diese Installationsanleitung
GuardLogix-Steuerung und DeviceNet-Geräten	1756-DNB	DNET-IN001
GuardLogix-Steuerung und EtherNet/IP-Geräten	1756-ENBT 1756-EN2T 1756-EN2F 1756-EN2TR 1756-EN3TR 1756-EN2TXT 1756-EN2TRXT	ENET-IN002
Steuerungen im ControlNet-Netzwerk	1756-CN2 1756-CN2R 1756-CN2RXT	CNET-IN005

Die GuardLogix-Steuerung kann eine Verbindung mit der Anwendung Logix Designer über einen USB-Anschluss, ein Ethernet-Modul oder ein ControlNet-Modul herstellen.

Weitere Informationen über Netzwerkkommunikationsmodule finden Sie unter Weitere Informationen auf Seite 14.

Programmieranforderungen

Ermitteln Sie anhand Tabelle 7 das Programmierwerkzeug (und die geeigneten Versionen), das zur Verwendung mit Ihrer GuardLogix-Steuerung der Serie 5570 zur Verfügung steht.

Tabelle 7 – Softwareversionen

Best.- Nr.	Studio 5000-Umgebung	Version Software RSLogix 5000(1)	Version Software RSLinx® Classic
1756-L71S, 1756-L72S, 1756-L73S, 1756-L73SXT	21 oder höher	20 oder höher	2.59 oder höher

(1) Informationen zur Verwendung einer GuardLogix-Steuerung mit der Software RSLogix 5000 finden Sie in der Publikation 1756-UM020, GuardLogix-Steuerungen – Benutzerhandbuch, und der Publikation 1756-RM093, GuardLogix Controller Systems Safety Reference Manual.

Sicherheitsroutinen umfassen Sicherheitsbefehle, die eine Untermenge des Standardbefehlssatzes für Kontaktplanlogik sind, sowie Befehle für Sicherheitsanwendungen. Unter der Sicherheits-Task geplante Programme unterstützen nur Kontaktplanlogik.

Tabelle 8 – Unterstützte Funktionen

Funktion	Anwendung Studio 5000 Logix Designer, Version 24 und höher	
	Sicherheits-Task	Standard-Task
Add-On-Befehle	x	x
Alarmmeldungen und Ereignisse		
Steuerungsprotokollierung	x	
Datenzugriffssteuerung		
Routinen der Gerätephase		
Ereignisgesteuerte Tasks		
Firmware Supervisor	x	
Funktionsblockdiagramme (FBD)		
Integrierte Achssteuerung		
Kontaktplanlogik	x	
Sprachenwechsel		
Speicherkarte		
Network Address Translation (NAT)		
Online-Import und -Export von Programmkomponenten		
Sicherheits- und Standardverbindungen	x	
Routinen in sequenzieller Ablaufsprache (SFC)		
Strukturierter Text		
Unicast-Verbindungen für produzierte und konsumierte Sicherheits-Tags	x	
Unicast-Verbindungen für Sicherheits-E/A-Geräte auf EtherNet/IP-Netzwerken		

Informationen zur Verwendung dieser Funktionen finden Sie in der Publikation 1756-PM001, Logix5000 Controllers Common Procedures Programming Manual, in den im Abschnitt Weitere Informationen auf Seite 14 genannten Publikationen und in der Online-Hilfe.

Notizen:

Installation der Steuerung

Thema	Seite
Vorsichtsmaßnahmen	25
Sicherstellen der Verfügbarkeit aller Komponenten	28
Installieren eines Chassis und eines Netzteils	29
Einsetzen der Steuerung in das Chassis	29
Einbauen oder Ausbauen einer Speicherkarte	31
Herstellen einer Kommunikationsverbindung	33
Update der Steuerung	36
Auswählen der Betriebsart der Steuerung	38
Deinstallieren eines Energiespeichermoduls (ESM)	39
Installieren eines Energiespeichermoduls (ESM)	41

Vorsichtsmaßnahmen

Lesen und befolgen Sie diese Vorsichtsmaßnahmen beim Einsatz der Ausrüstung.

Informationen über Umgebung und Gehäuse

ACHTUNG: Dieses Gerät wurde für den Einsatz in einer industriellen Umgebung mit einer Verschmutzung des Grades 2, in Anwendungen mit Überspannungskategorie II (gemäß IEC-Publikation 60664-1) und in Höhen von bis zu 2000 m ohne Minderung der Betriebswerte entwickelt.

Diese Anlage ist nicht für den Einsatz in Wohngebieten vorgesehen und bietet in solchen Umgebungen eventuell keinen ausreichenden Schutz für Funkkommunikationsdienste.

Dieses Gerät wird als „offenes" Gerät geliefert. Es muss in ein Gehäuse eingebaut werden, das für diese speziellen Umgebungsbedingungen zugelassen ist und den Zugriff auf leitfähige Teile und damit eher das Risiko von Verletzungen verhindert. Das Gehäuse muss über geeignete flammhemmende Eigenschaften verfügen, um die Ausbreitung von Flammen zu verhindern oder zu minimieren, und dabei die Flammenausbreitungsklassifizierung 5VA erfüllen. Sofern es nicht aus Metall besteht, muss das Gehäuse für die Anwendung genehmigt werden. Das Innere des Gehäuses darf nur unter Zuhilfenahme eines Werkzeugs zugänglich sein. Nachfolgende Abschnitte dieser Publikation können zusätzliche Informationen bezüglich der spezifischen Gehäuseschutzklassen enthalten, die erforderlich sind, um bestimmte Produktsicherheits-Zertifizierungen einzuhalten.

Lesen Sie zusätzlich zu dieser Publikation auch folgende Publikationen:

- Richtlinien zur störungsfreien Verdrahtung und Erdung von industriellen Automatisierungssystemen, Publikation 1770-4.1, mit Informationen zu zusätzlichen Installationsanforderungen
- NEMA-Norm 250 und IEC 60529, sofern zutreffend, mit Erklärungen zur Schutzklasse der verschiedenen Gehäuse

Programmierbare Elektroniksysteme (PES)

ACHTUNG: Personal, das für die Anwendung sicherheitsrelevanter programmierbarer Elektroniksysteme (PES) verantwortlich ist, muss mit den Sicherheitsanforderungen bei der Anwendung des Systems vertraut sein und für die Verwendung des Systems geschult sein.

Ziehen und Stecken unter Spannung

WARNUNG: Wenn Sie das Modul bei aktivierter Backplane einsetzen oder entfernen, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß. Verschlissene Kontakte können einen elektrischen Widerstand verursachen und den Modulbetrieb beeinträchtigen.

Zulassung für explosionsgefährdete Standorte – Nordamerika

The following information applies when operating this equipment in hazardous locations.	**Die folgenden Informationen gelten, wenn dieses Gerät an explosionsgefährdeten Standorten eingesetzt wird.**
Products marked "CL I, DIV 2, GP A, B, C, D" are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest "T" number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Produkte, die mit „CL I, DIV 2, GP A, B, C, D" gekennzeichnet sind, eignen sich nur für den Einsatz an explosionsgefährdeten Standorten der Klasse I, Division 2, Gruppe A, B, C, D, und an nicht explosionsgefährdeten Standorten. Bei allen Produkten ist auf dem Typenschild der Temperaturcode für den explosionsgefährdeten Standort angegeben. Werden Produkte innerhalb eines Systems kombiniert, kann anhand des ungünstigsten Temperaturcodes (niedrigste „T"-Zahl) der Temperaturcode für das gesamte System bestimmt werden. Gerätekombinationen in Ihrem System müssen bei der Installation durch die für Sie zuständige Behörde überprüft werden.
WARNING: EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**WARNUNG:** EXPLOSIONSGEFAHR • Geräte dürfen erst dann vom System getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt. • Verbindungen zu den Geräten dürfen erst dann getrennt werden, wenn die Stromversorgung unterbrochen wurde oder wenn es sich um einen bekanntermaßen nicht explosionsgefährdeten Bereich handelt. Sichern Sie alle externen Verbindungen zu diesem Gerät mit Schrauben, Schiebeverriegelungen, Gewindeanschlüssen oder anderen Vorrichtungen, die mit diesem Produkt geliefert werden. • Ein Austausch von Komponenten kann die Eignung für Klasse I, Division 2, beeinträchtigen. • Falls das Produkt Batterien enthält, dürfen diese nur in einem Bereich ausgetauscht werden, der bekanntermaßen nicht explosionsgefährdet ist.

Zulassung für explosionsgefährdete Standorte – Europa

Wenn das Produkt die Ex-Kennzeichnung trägt, gilt Folgendes.

Dieses Gerät ist für die Verwendung an explosionsgefährdeten Standorten gemäß der EU-Richtlinie 94/9/EG vorgesehen und wurde als konform mit den grundlegenden Gesundheits- und Sicherheitsanforderungen hinsichtlich des Designs und Aufbaus von Geräten der Kategorie 3 bewertet, die für die Verwendung an potenziell explosionsgefährdeten Standorten der Zone 2 gemäß Anhang II dieser Richtlinie vorgesehen sind.

Die Übereinstimmung mit den grundlegenden Gesundheits- und Sicherheitsanforderungen wurde durch die Konformität mit EN 60079-15 und EN 60079-0 versichert.

ACHTUNG: Dieses Gerät darf nicht direktem Sonnenlicht oder anderen Quellen mit UV-Strahlung ausgesetzt werden.

WARNUNG: Befolgen Sie bei der Montage und Verwendung dieses Geräts die folgenden Richtlinien:

- Dieses Gebereiche.
- Darf nur mit ATEX-zertifizierten Backplanes von Rockwell Automation verwendet werden.
- Geräte dürfen erst dann vom System getrennt werden, wenn die Stromverät muss bei Verwendung in Umgebungen der Zone 2 in einem ATEX-zertifizierten Gehäuse mit einer Mindestschutzart von IP54 (wie in IEC60529 definiert) montiert und in einer Umgebung mit einem Verschmutzungsgrad von maximal 2 eingesetzt werden (wie in IEC 60664-1 definiert). Abdeckungen oder Klappen des Gehäuses dürfen nur mit einem Werkzeug geöffnet werden können.
- Verwendung nur innerhalb der von Rockwell Automation angegebenen Leistungsrsorgung unterbrochen wurde oder wenn bekannt ist, dass es sich nicht um einen explosionsgefährdeten Bereich handelt.

Es müssen Vorsichtsmaßnahmen getroffen werden, um ein Überschreiten der Bemessungsspannung durch Einschwingstörungen von mehr als 140 % zu verhindern, wenn das Gerät in Umgebungen der Zone 2 eingesetzt wird.

Sichern Sie alle externen Verbindungen zu diesem Gerät mit Schrauben, Schiebeverriegelungen, Gewindeanschlüssen oder anderen Vorrichtungen, die mit diesem Gerät geliefert werden.

Verhindern elektrostatischer Entladung

ACHTUNG: Dieses Gerät ist empfindlich gegen elektrostatische Entladung, die interne Schäden verursachen und die normale Funktionsweise beeinträchtigen kann. Befolgen Sie beim Umgang mit diesem Gerät die folgenden Richtlinien:

- Berühren Sie einen geerdeten Gegenstand, um eventuelle elektrische Ladung abzuleiten.
- Tragen Sie ein zugelassenes Erdungsband am Handgelenk.
- Berühren Sie keine Anschlüsse oder Stifte auf den Komponentenplatinen.
- Berühren Sie keine Schaltkreiskomponenten im Innern des Geräts.
- Verwenden Sie möglichst einen vor statischen Entladungen sicheren Arbeitsplatz.
- Lagern Sie das Gerät in einer geeigneten antistatischen Verpackung, wenn Sie es nicht verwenden.

Sicherstellen der Verfügbarkeit aller Komponenten

Stellen Sie sicher, dass Sie über alle benötigten Komponenten verfügen, bevor Sie mit der Arbeit beginnen.

WICHTIG Sie müssen eine Primärsteuerung **und** einen Sicherheitspartner verwenden, um SIL 3/PLe zu erreichen.

Diese Teile sind im Lieferumfang von Primärsteuerung und Sicherheitspartner enthalten.

Best.- Nr.	Beschreibung	Im Lieferumfang enthalten
1756-L71S 1756-L72S 1756-L73S	Primärsteuerung	• 1756-ESMCAP – Kondensatorbasiertes Energiespeichermodul (ESM) • 1784-SD1 ? SD-Speicherkarte, 1 GB • 1747-KY ? Schlüssel
1756-L7SP	Sicherheitspartner	• 1756-SPESMNSE – Energiespeichermodul (ESM)
1756-L73SXT	Für extreme Temperaturen ausgelegte Primärsteuerung	• 1756-ESMCAPXT – Kondensatorbasiertes Energiespeichermodul (ESM) • 1747-KY – Schlüssel
1756-L7SPXT	Für extreme Temperaturen ausgelegter Sicherheitspartner	• 1756-SPESMNSEXT – Kondensatorbasiertes Energiespeichermodul (ESM)

Die folgende Ausrüstung kann optional eingesetzt werden.

Anforderung der Anwendung	Zu verwendendes Teil
Nichtflüchtiger Speicher	1784-SD1 (1 GB) oder 1784-SD2 (2 GB)
Abbau der gespeicherten Restenergie des installierten ESM auf 200 µJ oder weniger, bevor es in Ihre Anwendung integriert oder daraus ausgebaut werden kann(1)	1756-ESMNSE für die Primärsteuerung 1756-SPESMNSE für den Sicherheitspartner(2) Dieses ESM biete keine Backupleistung für die Uhrzeit. Zudem können Sie dieses ESM nur mit der Steuerung 1756-L73S (8 MB) oder mit einer Steuerung mit kleinerem Speicher verwenden.
Absicherung der Steuerung durch das ESM, das die Verwendung des USB-Ports und der SD-Karte verhindert(1)	1756-ESMNRM für die Primärsteuerung 1756-SPESMNRM für den Sicherheitspartner(3) Dieses ESM bietet Ihrer Anwendung eine höhere Sicherheit.

(1) Informationen zur Haltezeit der ESMs finden Sie im Abschnitt Abschätzen der ESM-Unterstützung für die Uhrzeit auf Seite 124.

(2) Für den Einsatz bei extremen Temperaturen ist 1756-ESMNSEXT für die Primärsteuerung und 1756-SPESMNSEXT für den Sicherheitspartner einzusetzen.

(3) Für den Einsatz bei extremen Temperaturen ist 1756-ESMNRMXT für die Primärsteuerung und 1756-SPESMNRMXT für den Sicherheitspartner einzusetzen.

Installieren eines Chassis und eines Netzteils

Sie müssen ein Chassis und ein Netzteil installieren, bevor Sie eine Steuerung einbauen.

1. Installieren Sie ein ControlLogix-Chassis gemäß der entsprechenden Installationsanleitung.

Best.- Nr.	Verfügbare Steckplätze	Serie	Siehe Installationsanleitung
1756-A4	4	B	1756-IN005
1756-A7	7		
1756-A10	10		
1756-A13	13		
1756-A17	17		
1756-A4LXT	4	B	
1756-A5XT	5	B	
1756-A7XT	7	B	
1756-A7LXT	7	B	

Steuerungen für den Einsatz unter extremen Umgebungsbedingungen (XT) benötigen ein XT-Chassis.

2. Installieren Sie ein ControlLogix-Netzteil gemäß der entsprechenden Installationsanleitung.

Best.- Nr.	Beschreibung	Serie	Siehe Installationsanleitung
1756-PA72	Netzteil, AC	C	1756-IN005
1756-PB72	Netzteil, DC		
1756-PA75	Netzteil, AC	B	
1756-PB75	Netzteil, DC		
1756-PAXT	XT-Netzteil, AC	B	
1756-PBXT	XT-Netzteil, DC		

Steuerungen für den Einsatz unter extremen Umgebungsbedingungen (XT) erfordern ein XT-Netzteil.

Einsetzen der Steuerung in das Chassis

Sie können eine Steuerung bei eingeschalteter Chassisspannungsversorgung und bei laufendem System ein- oder ausbauen.

WARNUNG: Wenn Sie das Modul einsetzen oder herausnehmen, während die Backplane eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

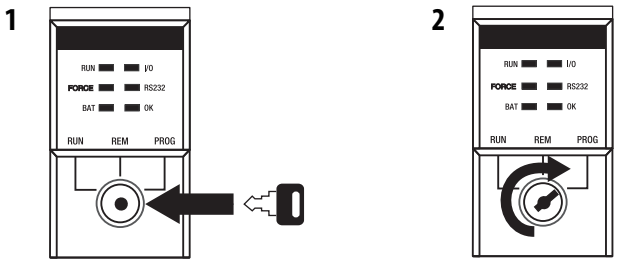
Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß. Abgenutzte Kontakte können einen elektrischen Widerstand verursachen und den Steuerungsbetrieb beeinträchtigen.

WICHTIG Das ESM beginnt in den folgenden Fällen mit der Aufladung:

- Die Steuerung und das ESM werden in ein an die Stromversorgung angeschlossenes Chassis installiert.
- Das Chassis, das die Steuerung mit dem installierten ESM enthält, wird eingeschaltet.
- Ein ESM wird in eine an die Stromversorgung angeschlossene Steuerung eingebaut.

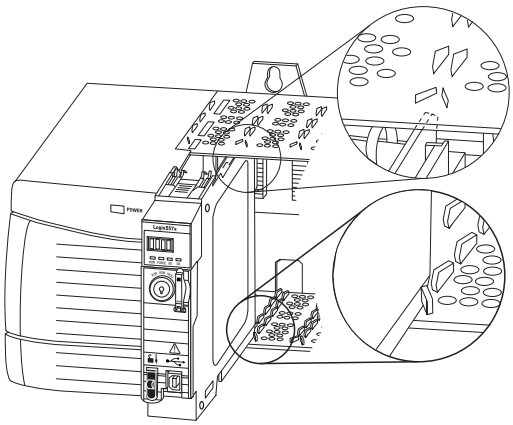
Nach dem Einschalten lädt das ESM etwa zwei Minuten lang, was durch die Meldung „CHRG“ (Aufladen) oder „ESM Charging“ (ESM aufladen) in der Statusanzeige bestätigt wird.

1. Führen Sie den Schlüssel in die Primärsteuerung ein.
2. Drehen Sie den Schlüssel in die Position „PROG“.



Der Sicherheitspartner verfügt über keinen Schlüsselschalter.

3. Richten Sie die Leiterplatte an den oberen und unteren Führungen im Chassis aus.



4. Schieben Sie die Steuerung in das Chassis.

Die Steuerung ist vollständig eingebaut, wenn sie bündig mit dem Netzteil und den anderen installierten Modulen abschließt sowie die oberen und unteren Verriegelungen eingerastet sind.

WICHTIG Der Sicherheitspartner muss im Steckplatz unmittelbar rechts neben die Primärsteuerung installiert werden. Führen Sie die oben beschriebenen Schritte 3 und 4 aus, um den Sicherheitspartner zu installieren.

Wenn Sie die Steuerung in das Chassis eingesetzt haben, lesen Sie den Abschnitt Kapitel 9, der weitere Informationen zur Interpretation der Statusleuchten der Primärsteuerung und des Sicherheitspartners enthält.

Einbauen oder Ausbauen einer Speicherkarte

WARNUNG: Wenn Sie die Speicherkarte bei eingeschaltetem System einsetzen oder herausnehmen, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden. Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

ACHTUNG: Wenn Sie **nicht** sicher sind, ob Inhalte auf der Speicherkarte gespeichert sind, drehen Sie **vor** der Installation der Karte den Steuerungsschlüsselschalter in die Position „PROG“. Abhängig vom Inhalt der Karte kann das Aus- und Einschalten der Versorgungsspannung oder ein Fehler dazu führen, dass die Karte ein anderes Projekt oder Betriebssystem in die Steuerung lädt.

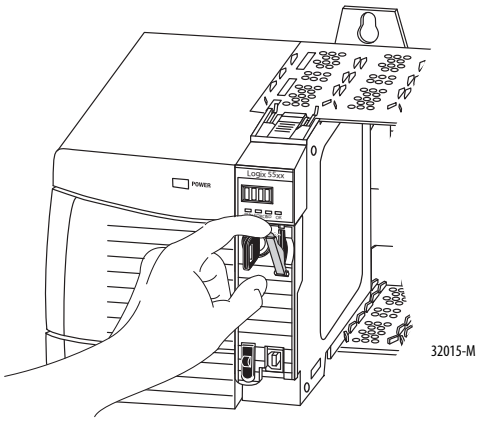
Im Lieferumfang der Steuerung ist eine bereits installierte SD-Karte enthalten. Es wird empfohlen, die SD-Karte installiert zu lassen.

Ausbauen der SD-Karte

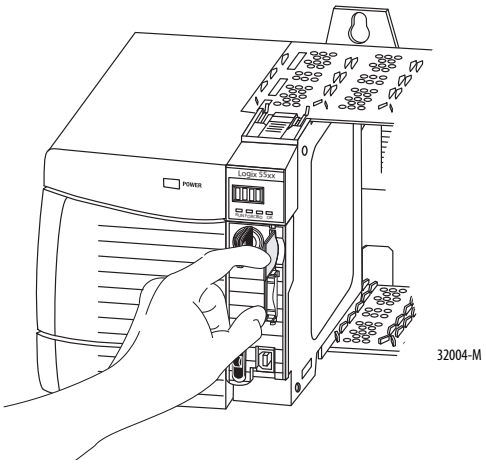
Gehen Sie wie folgt vor, um die SD-Karte zu entfernen.

WICHTIG Stellen Sie vor dem Ausbau der Karte sicher, dass die Statusleuchte der SD-Karte deaktiviert ist und dass die Karte nicht verwendet wird.

1. Drehen Sie den Schlüsselschalter in die Position „PROG“.
2. Öffnen Sie die Klappe, um auf die SD-Karte zugreifen zu können.



3. Drücken Sie kurz auf die SD-Karte, um sie auszuwerfen.

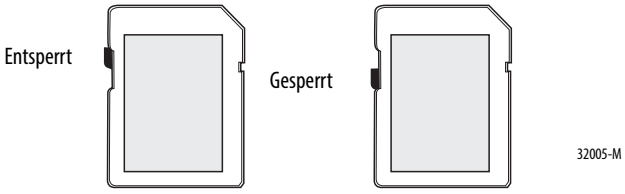


4. Nehmen Sie die SD-Karte heraus und schließen Sie die Klappe.

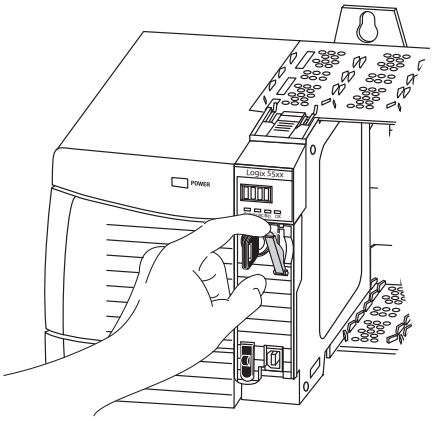
Einbauen der SD-Karte

Gehen Sie wie folgt vor, um die SD-Karte in die Steuerung einzubauen.

1. Vergewissern Sie sich, dass die SD-Karte, abhängig von Ihren Anforderungen, gesperrt oder entsperrt ist.

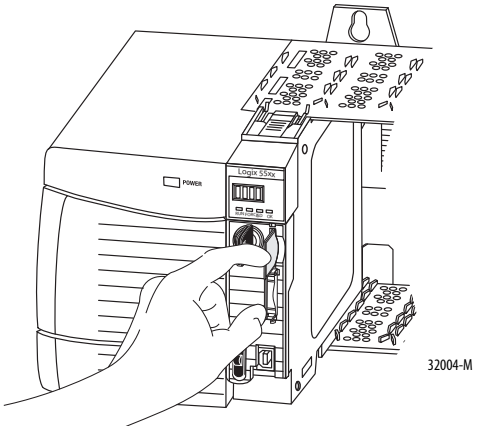


2. Öffnen Sie die Klappe für die SD-Karte.

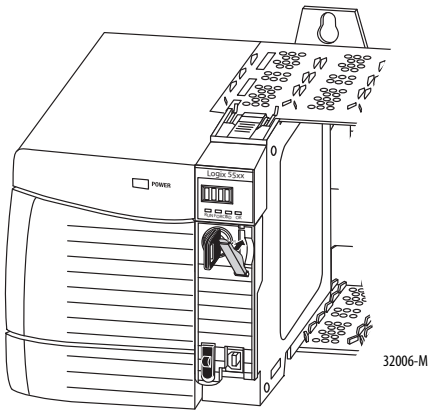


3. Setzen Sie die SD-Karte in den SD-Kartensteckplatz ein.

4. Drücken Sie die Karte vorsichtig in den Steckplatz, bis sie einrastet.



5. Schließen Sie die Klappe für die SD-Karte.



Herstellen einer Kommunikationsverbindung

Die Steuerung ist mit einem USB-Anschluss ausgestattet, der eine Buchse vom Typ B verwendet. Die Verbindung ist USB 2.0-kompatibel und überträgt Daten mit 12 Mbit/s.

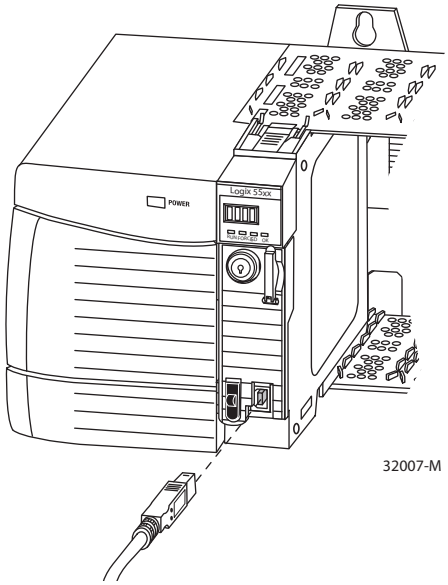
Wenn Sie den USB-Anschluss der Steuerung verwenden möchten, muss auf Ihrer Workstation die Software RSLinx, Version 2.59 oder höher, installiert sein. Verwenden Sie für den Anschluss Ihrer Workstation an den USB-Anschluss ein USB-Kabel. Mit dieser Verbindung können Sie direkt von der Workstation aus Firmware-Upgrades vornehmen und Programme auf die Steuerung herunterladen.

ACHTUNG: Verwenden Sie den USB-Anschluss für die temporäre lokale Programmierung. Verwenden Sie den USB-Anschluss nicht als dauerhafte Verbindung.

Das USB-Kabel darf maximal 3,0 m lang sein und darf keine Hubs umfassen.

WARNUNG: Verwenden Sie den USB-Anschluss nicht in explosionsgefährdeten Bereichen.

Abbildung 3 – USB-Anschluss



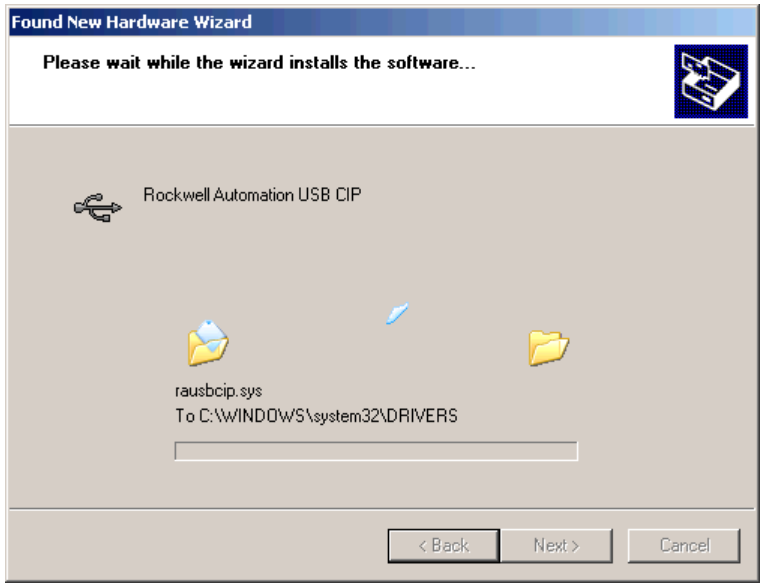
Wenn Sie die Software RSLinx so konfigurieren möchten, dass ein USB-Anschluss verwendet wird, müssen Sie zunächst einen USB-Treiber konfigurieren. Gehen Sie zum Konfigurieren eines USB-Treibers wie folgt vor.

1. Schließen Sie Ihre Steuerung und Workstation mithilfe eines USB-Kabels an.
2. Wählen Sie im Dialogfeld „Found New Hardware Wizard“ (Assistent für das Suchen neuer Hardware) eine der Optionen für Windows-Updates aus und klicken Sie auf „Next“ (Weiter).

HINWEIS Wenn die Software für den USB-Treiber nicht gefunden werden kann und die Installation abgebrochen wird, vergewissern Sie sich, dass die Software RSLinx Classic, Version 2.59 oder höher, installiert ist.

3. Klicken Sie auf „Install the software automatically (Recommended)“ (Software automatisch installieren (empfohlen)) und anschließend auf „Next“ (Weiter).

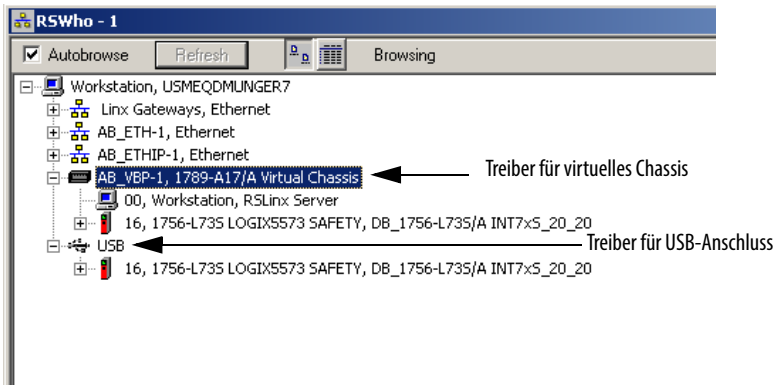
   Die Software wird installiert.



4. Klicken Sie auf „Finish“ (Fertigstellen), um Ihren USB-Treiber zu konfigurieren.

5. Um in der Software RSLinx direkt zu Ihrer Steuerung zu wechseln, klicken Sie auf das Symbol „RSWho“ .

   Im RSLinx-Workstation-Organisator wird Ihre Steuerung unter zwei verschiedenen Treibern angezeigt: unter einem virtuellen Chassis und unter dem USB-Anschluss. Sie können über beide Treiber zu Ihrer Steuerung wechseln.



Update der Steuerung

Im Lieferumfang der Steuerungen ist keine Firmware enthalten. Die Steuerungsfirmware wird im Paket mit der Studio 5000-Umgebung bereitgestellt. Zudem kann die Steuerungsfirmware auch von der Website von Rockwell Automation für technischen Support unter http://www.rockwellautomation.com/support/ heruntergeladen werden.

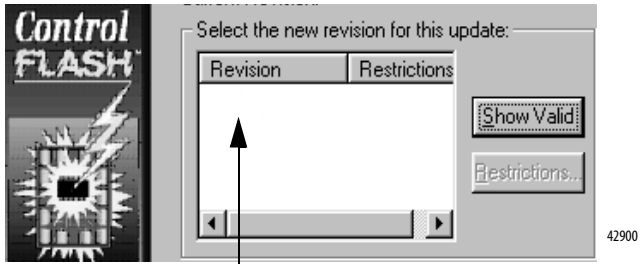
Sie können Ihre Steuerungsfirmware entweder mit der Software ControlFLASH™ oder mit der AutoFlash-Funktion der Anwendung Logix Designer aktualisieren.

Verwenden der Software ControlFLASH zum Aktualisieren der Firmware

Der Sicherheitspartner wird automatisch aktualisiert, wenn die Primärsteuerung aktualisiert wird.

WICHTIG	Wenn die SD-Karte gesperrt ist und die Option „Load Image“ (Abbilddatei laden) des gespeicherten Projekts auf „On Power Up“ (Beim Einschalten) gesetzt ist, wird die Steuerungsfirmware mit diesen Schritten nicht aktualisiert. Stattdessen werden die zuvor gespeicherte Firmware und das zuvor gespeicherte Projekt geladen.

1. Stellen Sie sicher, dass die entsprechende Netzwerkverbindung hergestellt wurde und dass der Netzwerktreiber in der Software RSLinx konfiguriert wurde.
2. Starten Sie die Software ControlFLASH.
3. Klicken Sie auf „Next“ (Weiter).
4. Wählen Sie die Bestellnummer Ihrer Steuerung aus und klicken Sie auf „Next“ (Weiter).
5. Erweitern Sie den Netzwerktreiber, bis Ihre Steuerung angezeigt wird.
6. Wählen Sie die Steuerung aus und klicken Sie auf „Next“ (Weiter).



7. Wählen Sie die Version für das Steuerungsupdate aus und klicken Sie auf „Next“ (Weiter).
8. Zum Starten des Updates der Steuerung klicken Sie auf „Finish“ (Fertigstellen) und anschließend auf „Yes“ (Ja).

Nach dem Update der Steuerung wird im Status-Dialogfeld „Update complete“ (Update abgeschlossen) angezeigt.

WICHTIG	Warten Sie, bis die Firmware vollständig aktualisiert wurde, bevor Sie das System aus- und wieder einschalten, und unterbrechen Sie das Update auch nicht auf andere Weise.

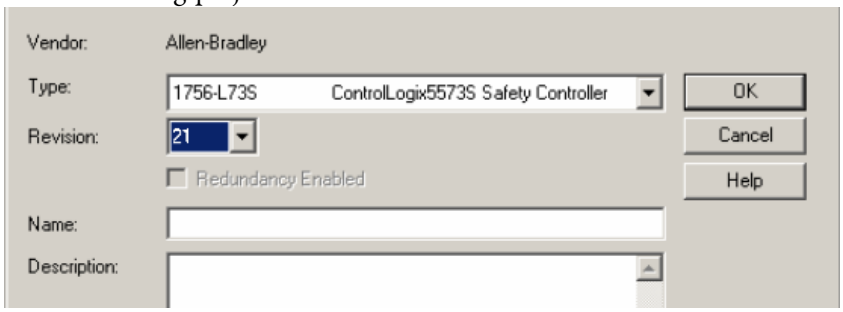
HINWEIS	Wenn das ControlFLASH-Update der Steuerung unterbrochen wird, kehrt die Steuerung wieder zur Boot-Firmware zurück, also zu Firmwareversion 1.*xxx*.

9. Klicken Sie auf „OK“.
10. Schließen Sie die Software ControlFLASH.

Verwenden von AutoFlash zum Aktualisieren der Firmware

Gehen Sie wie folgt vor, wenn Sie Ihre Steuerungsfirmware mit der AutoFlash-Funktion aktualisieren möchten.

1. Vergewissern Sie sich, dass die entsprechende Netzwerkverbindung hergestellt wurde und dass der Netzwerktreiber in der Software RSLinx konfiguriert wurde.
2. Verwenden Sie die Anwendung Logix Designer, um ein Steuerungsprojekt mit der für Sie erforderlichen Version zu erstellen.



3. Klicken Sie auf „RSWho“, um den Steuerungspfad anzugeben.

4. Wählen Sie Ihre Steuerung aus und klicken Sie auf „Update Firmware“ (Firmware aktualisieren).
5. Wählen Sie die gewünschte Firmwareversion aus.
6. Klicken Sie auf „Update“.
7. Klicken Sie auf „Yes“ (Ja).

Warten Sie, bis das Firmware-Update abgeschlossen wurde, ohne den Vorgang zu unterbrechen. Wenn das Firmware-Update abgeschlossen ist, wird das Dialogfeld „Who Active“ (Aktive Geräte) geöffnet. Sie können andere Tasks in der Anwendung Logix Designer ausführen.

Auswählen der Betriebsart der Steuerung

Bestimmen Sie anhand dieser Tabelle die Betriebsart Ihrer Steuerung.

Tabelle 9 – Betriebsarten der Steuerung

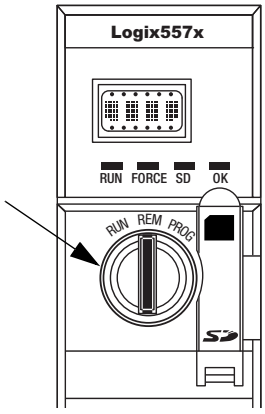
Gewünschte Funktionen	Wählen Sie eine dieser Betriebsarten aus				
	Run	Remote			Program
		Run	Test	Program	
Umschalten der Ausgänge in den von der Logik des Projekts vorgegebenen Zustand	x	x			
Umschalten der Ausgänge in ihren konfigurierten Zustand für den Programm-Modus			x	x	x
Ausführen (Abtasten) von Tasks	x	x	x		
Ändern der Betriebsart der Steuerung über die Anwendung Logix Designer		x	x	x	
Herunterladen eines Projekts		x	x	x	x
Planen eines ControlNet-Netzwerks				x	x
Bearbeiten des Projekts im Onlinezustand		x	x	x	x
Senden von Nachrichten	x	x	x		
Senden und Empfangen von Daten als Reaktion auf eine Nachricht von einer anderen Steuerung	x	x	x	x	x
Produzieren und Konsumieren von Tags	x	x	x	x	x

Ändern der Betriebsart über den Schlüsselschalter

Der Schlüsselschalter (Betriebsartschalter) an der Vorderseite der Steuerung kann zum Ändern der Betriebsart der Steuerung verwendet werden.
Die folgenden Betriebsarten stehen zur Auswahl:

- Programmierung (PROG)
- Dezentral (REM)
- Aktiv (RUN)

Abbildung 4 – Steuerungsschlüsselschalter



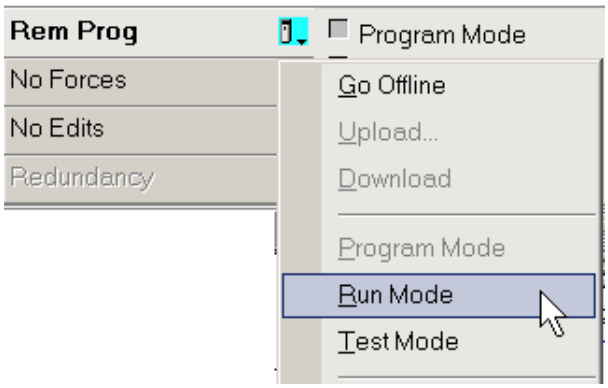
Ändern der Betriebsart über die Anwendung Logix Designer

Abhängig von der Steuerungsbetriebsart, die Sie mithilfe des Schlüsselschalters festlegen, können Sie die Betriebsart der Steuerung in der Anwendung Logix Designer ändern.

Wenn Sie die Steuerung im Online-Modus verwenden und sich der Steuerungsschlüsselschalter in der Position REM (mittlere Position) befindet, können Sie über das Menü „Controller Status“ (Steuerungsstatus) links oben im Anwendungsfenster des Logix Designer die folgenden Betriebsarten angeben:

- Remote Program
- Remote Run
- Remote Test

Abbildung 5 – Betriebsart über die Anwendung Logix Designer



HINWEIS Für dieses Beispiel wird mit dem Steuerungsschlüsselschalter die dezentrale Betriebsart (Remote-Modus) ausgewählt. Wenn mit Ihrem Steuerungsschlüsselschalter der Run-Modus oder Programm-Modus ausgewählt wird, ändern sich die Menüoptionen.

Deinstallieren eines Energiespeichermoduls (ESM)

Im Lieferumfang der Steuerungen ist bereits ein installiertes ESM enthalten.

Steuerung	Installierte ESM-Best.- Nr.
1756-L7xS, Steuerung	1756-ESMCAP
1756-L7xSXT, Steuerung für extreme Temperatur	1756-ESMCAPXT
1756-L7SP, Sicherheitspartner	1756-SPESMNSE
1756-L7SPXT, Sicherheitspartner für extreme Temperatur	1756-SPESMNSEXT

Beachten Sie vor dem Ausbau des ESM folgende Punkte:

- Wenn die Spannungsversorgung der Steuerung unterbrochen wird, entweder weil die Chassisspannung unterbrochen wurde oder die Steuerung aus einem eingeschalteten Chassis ausgebaut wurde, bauen Sie das ESM nicht sofort aus.

  Warten Sie, bis die Statusleuchte „OK“ der Steuerung von grün nach konstant rot wechselt und dann erlischt, bevor Sie das ESM ausbauen.

- Verwenden Sie das Modul 1756-ESMNSE, wenn für Ihre Anwendung das installierte ESM seine gespeicherte Restenergie auf 40 µJ oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr entfernt werden kann.
- Sobald es installiert ist, können Sie das Modul 1756-ESMNRM nicht aus der Steuerung ausbauen.

WICHTIG Stellen Sie vor dem Ausbau eines ESM Ihr Programm so ein, dass die möglichen Änderungen am Attribut „WallClockTime“ (Uhrzeit) berücksichtigt werden.

Gehen Sie wie folgt vor, um das Modul 1756-ESMCAP(XT), 1756-ESMNSE(XT) oder 1756-SPESMNSE(XT) aus der Steuerung auszubauen.

WARNUNG: Wenn für Ihre Anwendung das ESM seine gespeicherte Restenergie auf 40 µJoule oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr entfernt werden kann, müssen Sie ausschließlich das Modul 1756-ESMNSE(XT) für die Primärsteuerung und das Modul 1756-SPESMNSE(XT) für den Sicherheitspartner verwenden. Gehen Sie in diesem Fall wie folgt vor, bevor Sie das ESM ausbauen.

a. Schalten Sie die Chassisspannung aus.

   Nach dem Ausschalten der Chassisspannung wechselt die Statusleuchte „OK“ der Steuerung von grün nach konstant rot und erlischt dann.

b. Warten Sie **mindestens 20 Minuten**, bis die verbleibende gespeicherte Energie auf 40 µJ oder weniger abgebaut ist, bevor Sie das ESM ausbauen.

   Es erfolgt keine visuelle Anzeige, wenn die 20 Minuten abgelaufen sind. **Die Zeit muss von Ihnen selbst verfolgt werden**.

WARNUNG: Wenn Sie das Energiespeichermodul einsetzen oder herausnehmen, während die Backplane eingeschaltet ist, kann ein elektrischer Lichtbogen entstehen. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten. Wiederholte elektrische Lichtbogenbildung führt an den Kontakten des Moduls und des entsprechenden Anschlusses zu übermäßigem Verschleiß.

1. Ziehen Sie den Schlüssel vom Schlüsselschalter ab.

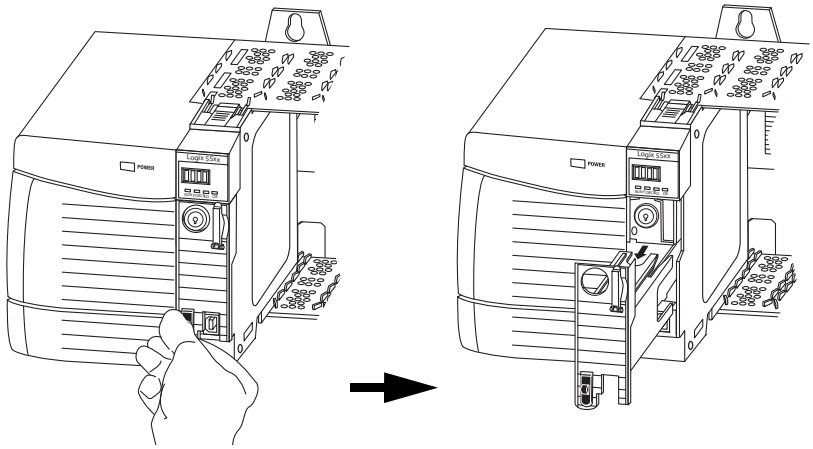
WICHTIG Der nächste Schritt ist abhängig von den Bedingungen, die für Ihre Anwendung gelten:

- Wenn Sie das ESM aus einer eingeschalteten Steuerung ausbauen, fahren Sie mit Schritt 2 fort.
- Wenn Sie das ESM aus einer Steuerung ausbauen, die nicht eingeschaltet ist – weil entweder die Chassisspannung ausgeschaltet ist oder die Steuerung aus einem eingeschalteten Chassis ausgebaut wurde – **, bauen Sie das ESM nicht sofort** aus.

  Warten Sie, bis die Statusleuchte „OK“ der Steuerung von grün nach konstant rot wechselt und dann erlischt, bevor Sie das ESM ausbauen.

  Wenn die Statusleuchte „OK“ erlischt, fahren Sie mit Schritt 2 fort.

2. Drücken Sie mit Ihrem Daumen auf die schwarze Entriegelung und ziehen Sie das ESM von der Steuerung weg.



Installieren eines Energiespeichermoduls (ESM)

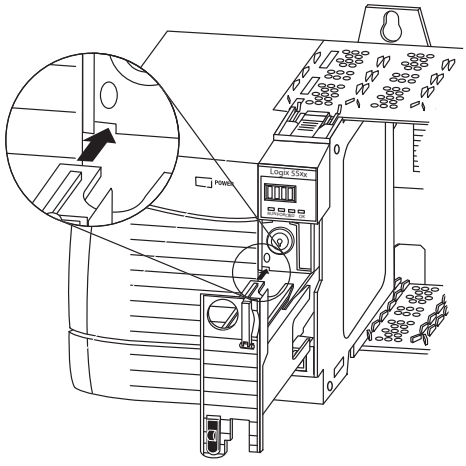
Tabelle 10 enthält eine Liste der ESMs und der kompatiblen GuardLogix-Steuerungen.

Tabelle 10 – Kompatible Energiespeichermodule

Best.- Nr.	Kompatible ESMs
1756-L7*x*S	1756-ESMCAP, 1756-ESMNSE, 1756-ESMNRM
1756-L7*x*SXT	1756-ESMCAPXT, 1756-ESMNSEXT, 1756-ESMNRMXT
1756-L7SP	1756-SPESMNSE, 1756-SPESMNRM
1756-L7SPXT	1756-SPESMNSEXT, 1756-SPESMNRMXT

Gehen Sie bei der Installation eines ESM wie folgt vor. Für den Sicherheitspartner ist die gleiche Vorgehensweise anzuwenden.

1. Richten Sie die Führungsschienen von ESM und Steuerung aus.



2. Schieben Sie das ESM in das Chassis, bis es einrastet.

ACHTUNG: Um mögliche Schäden am Produkt zu vermeiden, wenn Sie das ESM einsetzen, richten Sie es in der Führungsschiene aus und schieben Sie es mit minimalem Kraftaufwand nach vorne, bis es einrastet.

Das ESM beginnt unmittelbar nach der Installation mit dem Aufladen. Der Ladestatus wird durch eine der folgenden Statusmeldungen angezeigt:

- ESM Charging (ESM lädt auf)
- CHRG (Aufladen)

Nach der Installation des ESM kann es bis zu 15 Sekunden dauern, bis Meldungen zum Ladestatus angezeigt werden.

WICHTIG Warten Sie, bis das ESM aufgeladen ist, bevor Sie die Spannungsversorgung der Steuerung unterbrechen. Das ESM ist vollständig aufgeladen, wenn in der Statusanzeige die Meldung „CHRG“ (Aufladen) oder „ESM charging“ (ESM lädt auf) nicht mehr angezeigt wird.

HINWEIS Überprüfen Sie nach der Installation eines ESM die Attribute des Objekts „WallClockTime“ (Uhrzeit), um sicherzustellen, dass die Uhrzeit der Steuerung korrekt eingestellt ist.

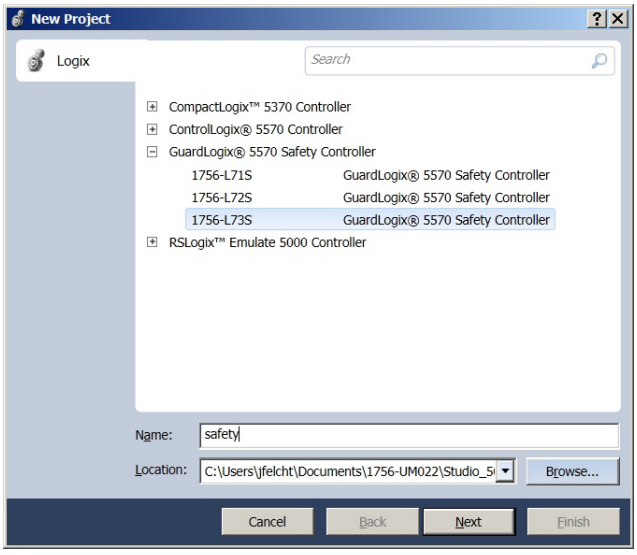
Konfiguration der Steuerung

Thema	Seite
Erstellen eines Steuerungsprojekts	43
Elektronische Codierung	46
Festlegen von Kennwörtern für die Sicherheitssperrung-und -entsperrung	47
Schützen der Sicherheits-Task-Signatur im Run-Modus	47
Austausch eines E/A-Geräts	48
Aktivieren der Zeitsynchronisierung	49
Konfigurieren einer Peer-Sicherheitssteuerung	50

Erstellen eines Steuerungsprojekts

Zur Konfiguration und Programmierung Ihrer Steuerung verwenden Sie die Anwendung Logix Designer, mit der Sie ein Projekt für die Steuerung erstellen und verwalten können.

1. Klicken Sie auf der Hauptsymbolleiste auf die Schaltfläche „New“ (Neu), um ein Projekt zu erstellen.
2. Doppelklicken Sie auf GuardLogix® 5570 Safety Controller, um die Liste der Steuerungsoptionen anzuzeigen.
3. Wählen Sie eine GuardLogix-Steuerung aus:
   - 1756-L71S GuardLogix® 5570 Safety Controller
   - 1756-L72S GuardLogix® 5570 Safety Controller
   - 1756-L73S GuardLogix® 5570 Safety Controller

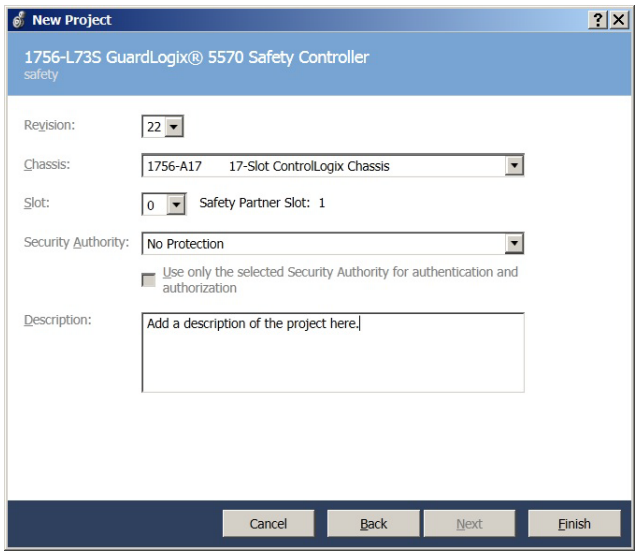


4. Geben Sie im Feld „Name“ den Namen des Projekts ein.
5. Klicken Sie auf „Browse“ (Durchsuchen), um den Ordner anzugeben, in dem das Sicherheitssteuerungsprojekt gespeichert werden soll.
6. Klicken Sie auf „Next“ (Weiter).

7. Wählen Sie im Menü „Revision“ (Version) die Hauptversion der Firmware für die Steuerung aus.
8. Wählen Sie im Menü „Chassis“ eine Chassisgröße aus.
9. Wählen Sie im Menü „Slot“ (Steckplatz) einen Steckplatz für den Sicherheitspartner aus.

   Das Dialogfeld „New Project“ (Neues Projekt) zeigt die Steckplatzposition des Sicherheitspartners basierend auf der für die Primärsteuerung eingegebenen Steckplatznummer an.

   Falls Sie eine Steckplatznummer für die Primärsteuerung wählen, die keinen Platz für den Sicherheitspartner direkt rechts neben der Primärsteuerung bietet, werden Sie aufgefordert, erneut eine gültige Steckplatznummer einzugeben.



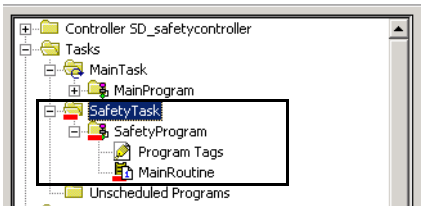
10. Wählen Sie im Menü „Security Authority“ (Sicherheitsberechtigung) eine Option aus.

    Ausführliche Informationen zu Sicherheitsfunktionen finden Sie in der Publikation 1756-PM016, Logix5000-Steuerungen – Sicherheit – Programmierhandbuch.

11. Aktivieren Sie das Kontrollkästchen unter „Security Authority“ (Sicherheitsberechtigung), wenn Sie den ausgewählten Schutz für die Authentifizierung und Autorisierung verwenden möchten.
12. Geben Sie im Feld „Description“ (Beschreibung) eine Beschreibung des Projekts ein.
13. Klicken Sie auf „Finish“ (Fertigstellen).

Die Anwendung Logix Designer generiert eine Sicherheits-Task und ein Sicherheitsprogramm. Eine Hauptroutine in Kontaktplanlogik, „MainRoutine“ genannt, wird ebenfalls innerhalb des Sicherheitsprogramms erstellt.

Abbildung 6 – Sicherheits-Task im Controller Organizer (Steuerungsorganisator)



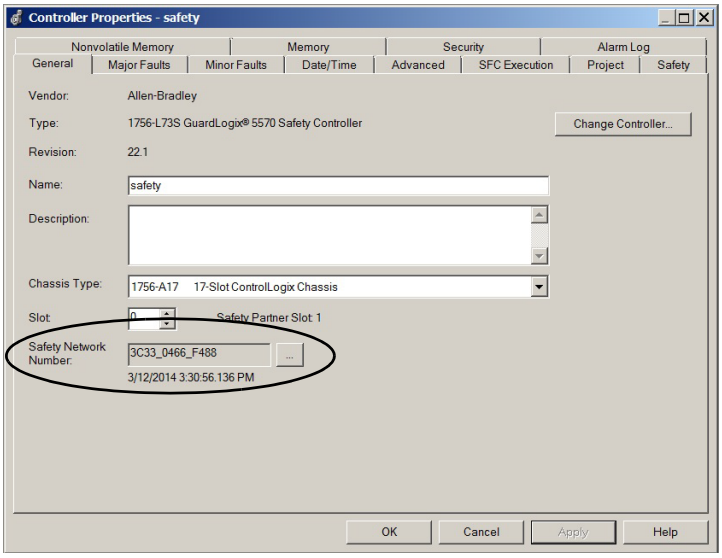
Ein roter Balken unter dem Ordnersymbol unterscheidet die Sicherheitsprogramme und -routinen von Standardkomponenten des Projekts im Controller Organizer (Steuerungsorganisator).

Wenn ein neues Sicherheitsprojekt angelegt wird, erstellt die Anwendung Logix Designer automatisch auch eine zeitbasierende Sicherheitsnetzwerknummer (SNN).

Diese SNN definiert die lokale Chassis-Backplane als Sicherheits-Subnetz. Sie kann über die Registerkarte „General“ (Allgemein) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) angezeigt und geändert werden.

Für die meisten Anwendungen ist diese automatische, zeitbasierende SNN ausreichend. Es gibt jedoch Fälle, in denen die Eingabe einer bestimmten SNN erforderlich ist.

Abbildung 7 – Sicherheitsnetzwerknummer



HINWEIS Sie können im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) die Steuerung von Standard auf Sicherheit oder Sicherheit auf Standard umschalten. Klicken Sie dazu auf die Schaltfläche „Change Controller“ (Steuerung ändern). Standard- und Sicherheitsprojekte werden dadurch jedoch wesentlich beeinflusst.

Ausführliche Informationen zu den Auswirkungen von Änderungen an der Steuerung finden Sie in Anhang B, Wechsel des Steuerungstyps.

Tabelle 11 – Weitere Informationen

Quelle	Beschreibung
Kapitel 6, Entwicklung von Sicherheitsanwendungen	Enthält weitere Informationen zu Sicherheits-Tasks, Sicherheitsprogrammen und Sicherheitsroutinen.
Kapitel 4, Kommunikation über Netzwerke	Bietet weitere Informationen zum Verwalten der SNN.

Elektronische Codierung

Mit der elektronischen Codierung wird die Wahrscheinlichkeit verringert, dass das falsche Gerät in einem Steuerungssystem verwendet wird. Damit wird das im Projekt definierte Gerät mit dem installierten Gerät verglichen. Wenn die Codierung nicht übereinstimmt, tritt ein Fehler auf. Folgende Attribute werden verglichen.

Attribut	Beschreibung
Vendor (Anbieter)	Der Gerätehersteller.
Device Type (Gerätetyp)	Der allgemeine Produkttyp, beispielsweise Digital-E/A-Modul.
Product Code (Produktcode)	Der spezifische Produkttyp. Der Produktcode entspricht einer Bestellnummer.
Major Revision (Hauptversion)	Eine Nummer, die den Funktionsumfang eines Geräts angibt.
Minor Revision (Nebenversion)	Eine Nummer, die Verhaltensänderungen des Geräts angibt.

Die folgenden Optionen sind für die elektronische Codierung verfügbar.

Codierungs-option	Beschreibung
Compatible Module (Kompatibles Modul)	Damit kann das installierte Gerät die Codierung des im Projekt definierten Geräts akzeptieren, sofern das installierte Gerät das definierte Gerät emulieren kann. Mit „Compatible Module“ kann ein Gerät durch ein anderes Gerät ersetzt werden, wenn letzteres die folgenden Merkmale hat: • Dieselbe Bestellnummer • Dieselbe oder eine höhere Hauptversion • Eine Nebenversion mit folgenden Bedingungen: – Wenn die Hauptversion identisch ist, muss die Nebenversion gleich oder höher sein. – Wenn die Hauptversion höher ist, spielt die Nebenversion keine Rolle.
Exact Match (Exakte Übereinstimmung)	Gibt an, dass für eine Kommunikation alle Codierungsattribute übereinstimmen müssen. Wenn eines der Attribute nicht exakt übereinstimmt, ist keine Kommunikation mit dem Gerät möglich. „Exact Match“ ist erforderlich, wenn Firmware Manager verwendet wird.

Bedenken Sie die Auswirkungen der Codierungsoptionen bei der Auswahl.

WICHTIG Wenn die elektronischen Codierungsparameter während des Betriebs geändert werden, werden die Verbindungen mit dem Gerät und allen am Gerät angeschlossenen Geräten unterbrochen. Verbindungen mit anderen Steuerungen können ebenfalls unterbrochen werden.

Wenn eine E/A-Verbindung mit einem Gerät unterbrochen wird, kann dies zu Datenverlust führen.

Weitere Informationen

Weitere Informationen zur elektronischen Codierung finden Sie in der Publikation LOGIX-AT001, Electronic Keying in Logix5000 Control Systems Application Technique.

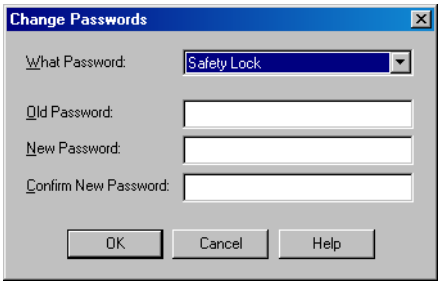
Festlegen von Kennwörtern für die Sicherheitssperrung-und -entsperrung

Die Sicherheitssperrung der Steuerung schützt Sicherheits-Steuerungskomponenten vor Änderungen. Nur Sicherheitskomponenten wie die Sicherheits-Task, die Sicherheitsprogramme, die Sicherheitsroutinen und die Sicherheits-Tags sind davon betroffen. Standardkomponenten sind nicht betroffen. Sie können die Sicherheitssperrung oder -entsperrung des Steuerungsprojekts entweder online oder offline durchführen.

Die Funktion zur Sicherheitssperrung und -entsperrung verwendet zwei getrennte Kennwörter. Kennwörter sind optional.

Gehen Sie zum Festlegen von Kennwörtern wie folgt vor:

1. Klicken Sie auf „Tools“ (Extras) > „Safety“ (Sicherheit) > „Change Passwords“ (Kennwörter ändern).
2. Wählen Sie im Pulldown-Menü „What Password“ (Welches Kennwort) entweder „Safety Lock“ (Sicherheitssperrung) oder „Safety Unlock“ (Sicherheitsentsperrung) aus.



3. Geben Sie das alte Kennwort ein, falls vorhanden.
4. Geben Sie anschließend das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf „OK“.

   Kennwörter können 1 bis 40 Zeichen lang sein und es wird nicht zwischen Klein- und Großbuchstaben unterschieden. Es können Buchstaben, Zahlen und die folgenden Zeichen verwendet werden: ‘ ~ ! @ # $ % ^ & * ( ) _ + , - = { } | [ ] \ : ; ? / .

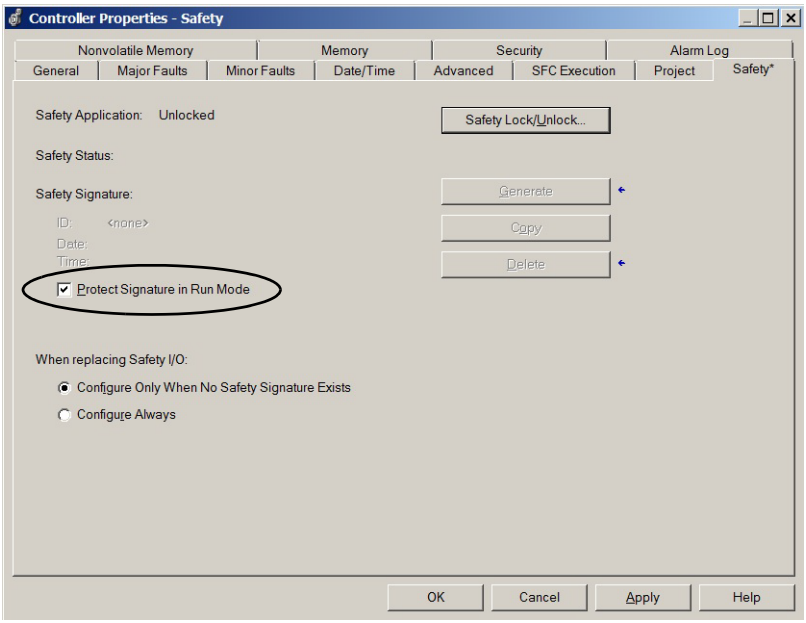
Schützen der Sicherheits-Task-Signatur im Run-Modus

Sie können verhindern, dass die Sicherheits-Task-Signatur erstellt oder gelöscht wird, während sich die Steuerung im Run- oder Remote-Run-Modus befindet, gleichgültig, ob die Sicherheitsanwendung gesperrt oder entsperrt ist.

Gehen Sie folgendermaßen vor, um die Sicherheits-Task-Signatur zu schützen:

1. Öffnen Sie das Dialogfeld „Controller Properties“ (Steuerungseigenschaften).
2. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).
3. Aktivieren Sie die Option „Protect Signature in Run Mode“ (Signatur im Run-Modus schützen).

4. Klicken Sie auf „OK“.



Austausch eines E/A-Geräts

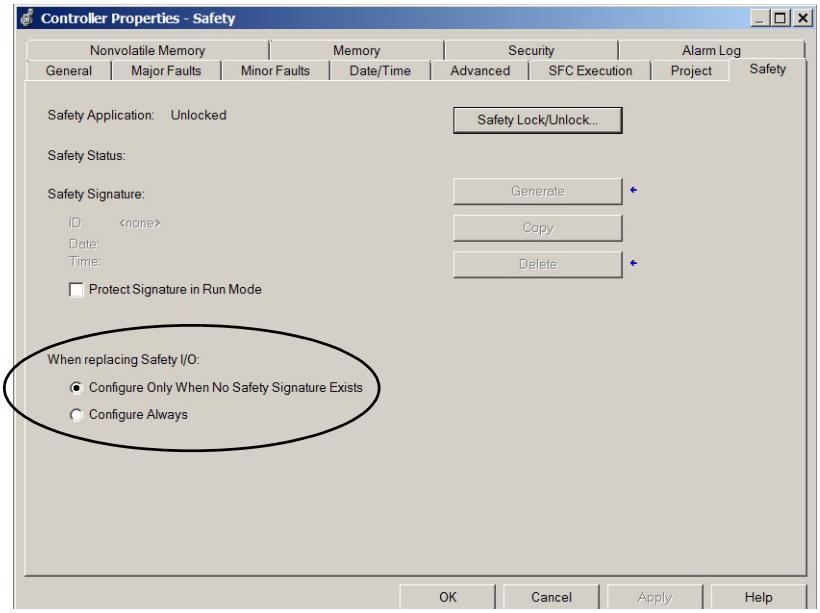
Mithilfe der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) können Sie definieren, wie die Steuerung den Austausch eines E/A-Geräts im System handhabt. Diese Option legt fest, ob die Steuerung die Sicherheitsnetzwerknummer (SNN) eines E/A-Geräts bestimmt, mit dem sie verbunden ist und für das sie Konfigurationsdaten besitzt, wenn eine Sicherheits-Task-Signatur(1) vorliegt.

Gehen Sie folgendermaßen vor, um zu konfigurieren, wie die Steuerung den Austausch eines E/A-Geräts im System handhabt.

1. Öffnen Sie das Dialogfeld „Controller Properties“ (Steuerungseigenschaften).
2. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).
3. Wählen Sie die Konfigurationsoption für die Steuerung aus, die beim Austausch der Sicherheits-E/A verwendet werden soll.
4. Klicken Sie auf „OK“.

(1) Die Sicherheits-Task-Signatur ist eine Nummer, die ausschließlich dazu verwendet wird, um Logik, Daten und Konfiguration jedes Projekts zu kennzeichnen und dadurch die Safety Integrity Level (SIL) des Systems zu schützen. Weitere Informationen finden Sie unter Sicherheits-Task-Signatur auf Seite 18 und Erstellen einer Sicherheits-Task-Signatur auf Seite 108.

Abbildung 8 – Optionen für den Austausch eines E/A-Geräts



ACHTUNG: Aktivieren Sie das Optionsfeld „Configure Always“ (Immer konfigurieren) nur, wenn die Beibehaltung von SIL 3 während des Austauschs und der Funktionstests eines Geräts nicht vom gesamten routbaren CIP-Safety-Steuerungssystem abhängt.

Weitere Informationen finden Sie in Kapitel 5, Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen.

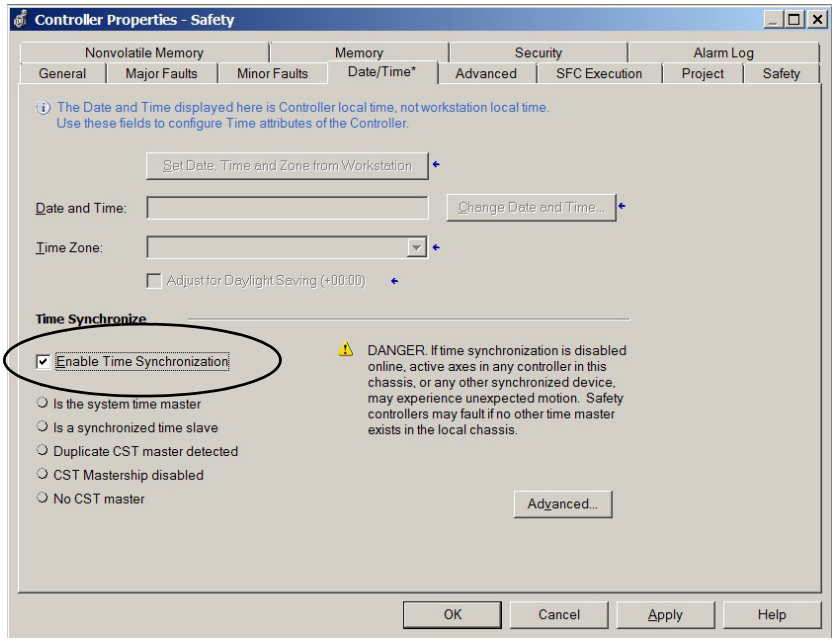
Aktivieren der Zeitsynchronisierung

In einem GuardLogix-Steuerungssystem muss ein Gerät im lokalen Chassis als Master für die koordinierte Systemzeit (CST-Master) festgelegt werden. Mit der Option „Time Synchronization“ (Zeitsynchronisierung) steht ein Standardmechanismus zum Synchronisieren der Uhren in einem Netzwerk mit dezentralen Geräten zur Verfügung.

Gehen Sie folgendermaßen vor, um die Steuerung als CST-Master zu konfigurieren.

1. Öffnen Sie das Dialogfeld „Controller Properties“ (Steuerungseigenschaften).
2. Klicken Sie auf die Registerkarte „Date/Time“ (Datum/Uhrzeit).
3. Aktivieren Sie die Option „Enable Time Synchronization“ (Zeitsynchronisierung aktivieren).
4. Klicken Sie auf „OK“.

Abbildung 9 – Registerkarte „Date/Time“ (Datum/Uhrzeit)



Weitere Informationen zur Zeitsynchronisierung finden Sie in der Publikation IA-AT003, Integrated Architecture and CIP Sync Configuration Application Solution.

Konfigurieren einer Peer-Sicherheitssteuerung

Sie können eine Peer-Sicherheitssteuerung zum E/A-Konfigurationsordner Ihres Sicherheitsprojekts hinzufügen, um zuzulassen, dass Standard- oder Sicherheits-Tags konsumiert werden. Zum Austausch von Sicherheitsdaten zwischen Peer-Steuerungen produzieren und konsumieren Sie Steuerungsbereichs-Sicherheits-Tags.

Einzelheiten zum Konfigurieren der Peer-Sicherheitssteuerungen sowie zum Produzieren und Konsumieren von Sicherheits-Tags siehe Produzierte/konsumierte Sicherheits-Tags auf Seite 98.

Kommunikation über Netzwerke

Thema	Seite
Das Sicherheitsnetzwerk	51
EtherNet/IP-Kommunikation	57
ControlNet-Kommunikation	62
DeviceNet-Kommunikation	64

Das Sicherheitsnetzwerk

Das CIP Safety-Protokoll ist ein Endknoten-zu-Endknoten-Sicherheitsprotokoll, welches das Routing von CIP Safety-Nachrichten zu und von Sicherheits-E/A-Geräten über Bridges, Switches und Router ermöglicht.

Um die hohe Integrität beizubehalten, wenn das Routing über Standard-Bridges, -Switches oder -Router erfolgt, muss jeder Endknoten innerhalb eines routingfähigen CIP Safety-Steuerungssystems über eine eindeutige Referenz verfügen. Diese eindeutige Referenz ist eine Kombination aus Sicherheitsnetzwerknummer (SNN) und der Netzknotenadresse des Netzwerkgeräts.

Verwalten der Sicherheitsnetzwerknummer

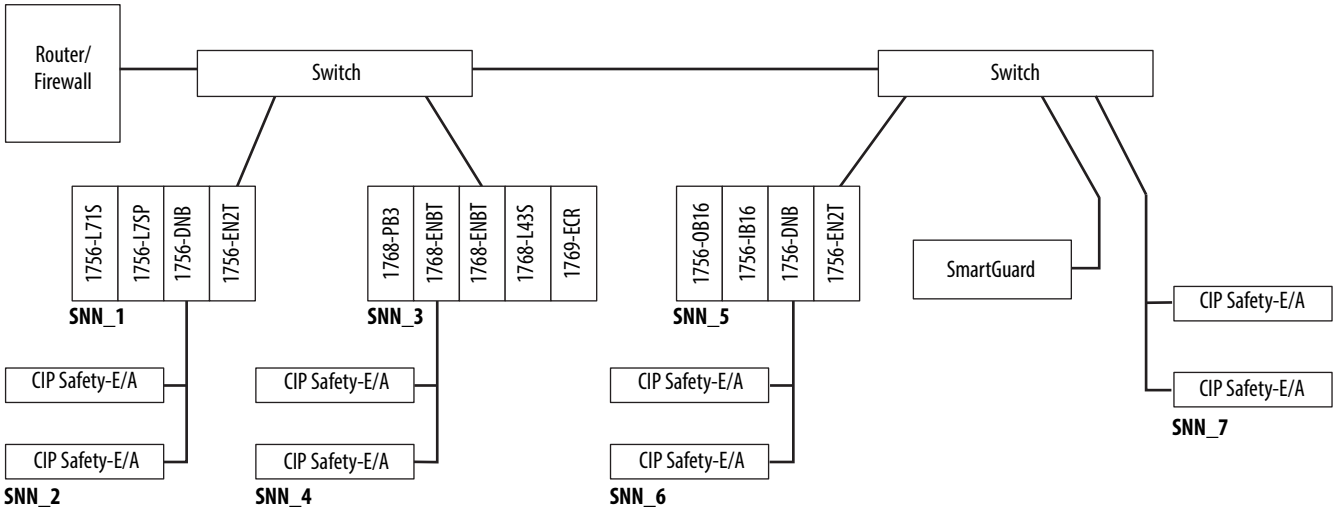
Sicherheitsnetzwerknummern (SNN), die Sicherheitsgeräten in einem Netzwerksegment zugeordnet werden, müssen eindeutig sein. Es muss sichergestellt werden, dass eine eindeutige SNN folgenden Elementen zugewiesen wird:

- jedem CIP Safety-Netzwerk, das Sicherheitsgeräte enthält.
- jedem Chassis, das mindestens eine GuardLogix-Steuerung enthält.

HINWEIS Mehrere Sicherheitsnetzwerknummern können einem CIP Safety-Subnetz oder einem ControlBus-Chassis zugeordnet werden, das mehr als ein Sicherheitsgerät enthält. Aus Gründen der Einfachheit wird jedoch empfohlen, jedem CIP Safety-Subnetz nur eine eindeutige SNN zuzuweisen.

In Abbildung 10 ist ein CIP-Sicherheitssystem mit sieben unterschiedlichen Subnetzen dargestellt, von denen jedes über eine eindeutige SNN verfügt.

Abbildung 10 – CIP-Sicherheitsbeispiel mit mehreren SNNs

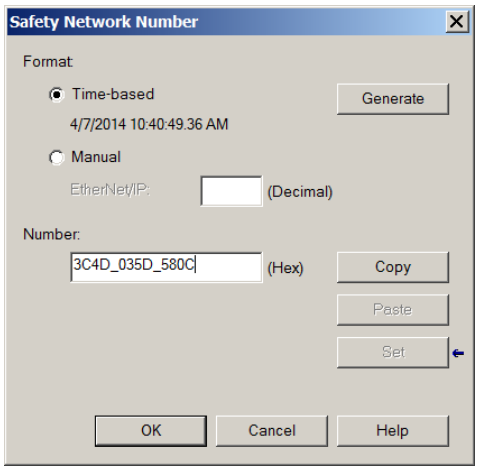


Die SNN kann von der Software (zeitbasiert) oder vom Anwender (manuell) zugewiesen sein. Diese beiden Formate einer SNN werden in den nachfolgenden Abschnitten beschrieben.

Zeitbasierte Sicherheitsnetzwerknummer

Wenn das zeitbasierte Format gewählt wird, repräsentiert der SNN-Wert Datum und Uhrzeit der Nummernerstellung, und zwar entsprechend dem Computer, auf dem die Konfigurationssoftware ausgeführt wird.

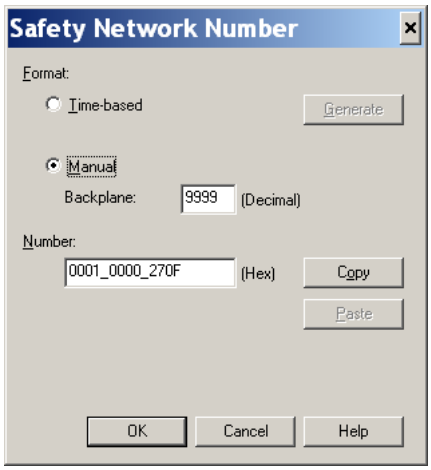
Abbildung 11 – Zeitbasiertes Format



Manuelle Sicherheitsnetzwerknummer

Wird das manuelle Format gewählt, wird die SNN als Wert von 1 bis 9999 dezimal eingegeben.

Abbildung 12 – Manuelle Eingabe



Zuordnen der Sicherheitsnetzwerknummer (SNN)

Sie können zulassen, dass die Anwendung Logix Designer eine SNN automatisch zuordnet, oder Sie können die SNN manuell zuweisen.

Automatische Zuweisung

Wenn eine neue Steuerung oder ein neues Gerät angelegt wird, wird eine zeitbasierte SNN automatisch zugewiesen. Werden zu einem späteren Zeitpunkt neue Sicherheitsgeräte zum gleichen CIP Safety-Netzwerk hinzugefügt, wird ihnen die gleiche SNN zugeordnet, die innerhalb der niedrigsten Adresse auf diesem CIP Safety-Netzwerk definiert ist.

Manuelle Zuweisung

Die manuelle Option ist für routingfähige CIP Safety-Systeme vorgesehen, die nur über wenige Netzwerk-Subnetze und zwischengeschaltete Netzwerke verfügen und bei denen die Anwender die SNN in einer logischen, der spezifischen Anwendung entsprechenden Art und Weise verwalten und zuweisen möchten.

Siehe Ändern der Sicherheitsnetzwerknummer (SNN) auf Seite 54.

WICHTIG Wenn Sie eine SNN manuell zuordnen, vergewissern Sie sich, dass die Systemerweiterung nicht zu einer Verdoppelung der Kombinationen aus SNN und Netzknotenadresse führt.

In Logix Designer, Version 24, tritt ein Verifizierungsfehler auf, wenn das Projekt doppelte SNN- und Knotenadressenkombinationen enthält.

In Logix Designer, Version 26, wird ein Warnfehler angezeigt, wenn das Projekt doppelte SNN- und Knotenadressenkombinationen enthält. Sie können das Projekt dennoch bestätigen, Rockwell Automation empfiehlt jedoch, die doppelten Kombinationen zu beheben.

Automatisch versus manuell

Für die meisten Anwender ist in der Regel die automatische Zuweisung einer SNN ausreichend. Allerdings ist eine manuelle Einstellung der SNN in den folgenden Situationen erforderlich:

- wenn konsumierte Sicherheits-Tags verwendet werden
- wenn das Projekt Sicherheitseingangsdaten von einem Modul konsumiert, dessen Konfiguration von einem anderen Gerät verwaltet wird
- wenn ein Sicherheitsprojekt in eine andere Hardwareinstallation innerhalb des gleichen routingfähigen CIP Safety-Systems kopiert wird

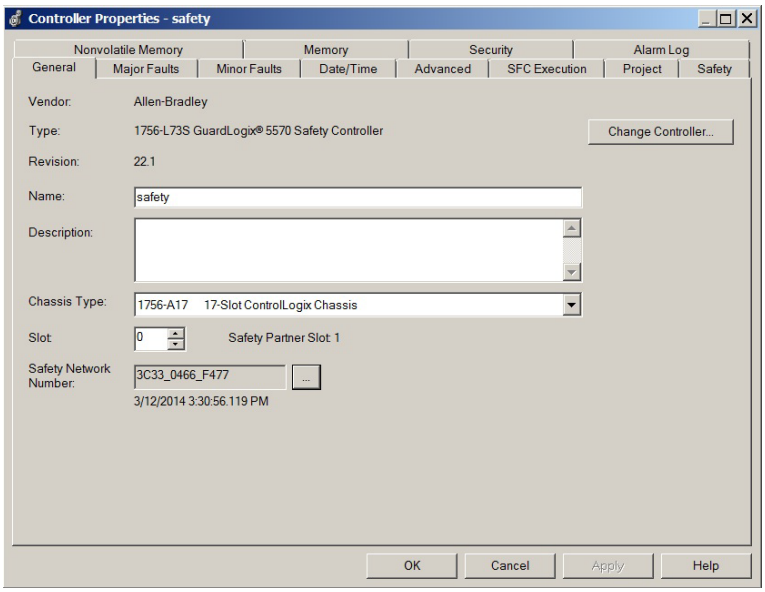
Ändern der Sicherheitsnetzwerknummer (SNN)

Bevor Sie die SNN ändern, müssen Sie folgende Maßnahmen durchführen:

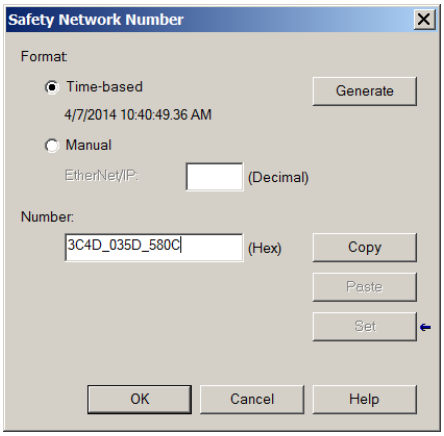
- Das Projekt entsperren, wenn es sicherheitsgesperrt ist.
  Siehe Sicherheitssperre der Steuerung auf Seite 106.
- Die Sicherheits-Task-Signatur löschen, sofern eine solche vorliegt.
  Siehe Löschen der Sicherheits-Task-Signatur auf Seite 109.

Ändern der Sicherheitsnetzwerknummer der Steuerung

1. Klicken Sie im Controller Organizer (Steuerungsorganisator) mit der rechten Maustaste auf die Steuerung und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf der Registerkarte „General“ (Allgemein) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf die Schaltfläche ... rechts neben „Safety Network Number“ (Sicherheitsnetzwerknummer), um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) zu öffnen.



3. Klicken Sie auf „Time-based“ (Zeitbasiert) und anschließend auf „Generate“ (Generieren).

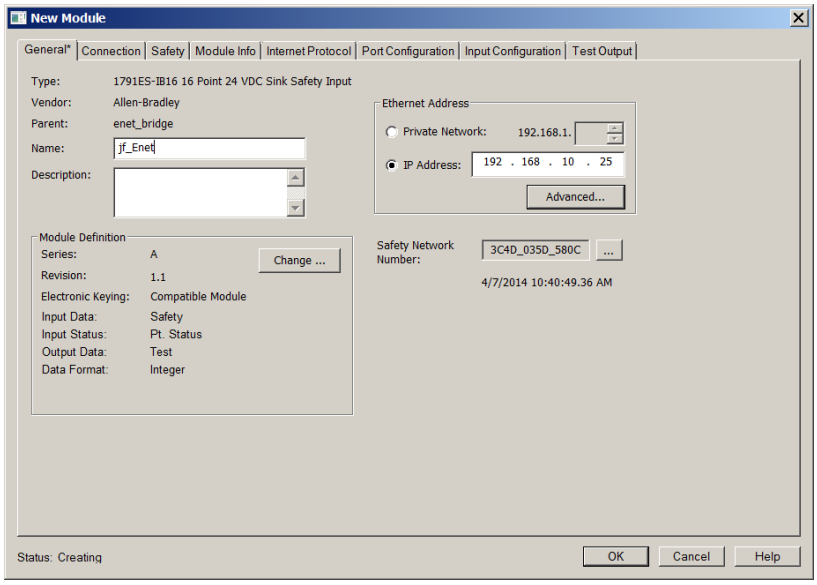


4. Klicken Sie auf „OK“.

Ändern der Sicherheitsnetzwerknummer eines Sicherheits-E/A-Geräts im CIP Safety-Netzwerk

In diesem Beispiel wird ein EtherNet/IP-Netzwerk verwendet.

1. Suchen Sie das erste EtherNet/IP-Kommunikationsmodul im E/A-Konfigurationsverzeichnis.
2. Erweitern Sie die über das EtherNet/IP-Kommunikationsmodul verfügbaren Sicherheits-E/A-Geräte.
3. Doppelklicken Sie auf das erste Sicherheits-E/A-Gerät, um die Registerkarte „General“ (Allgemein) aufzurufen.



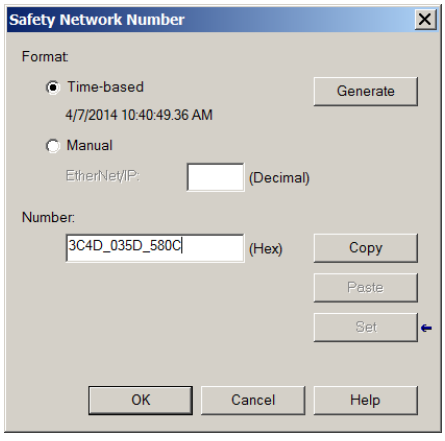
4. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche [...], um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.
5. Wählen Sie „Time-based“ (Zeitbasiert) und klicken Sie auf „Generate“ (Generieren), um eine neue SNN für dieses EtherNet/IP-Netzwerk zu erstellen.

6. Klicken Sie auf „OK“.
7. Klicken Sie auf die Schaltfläche „Copy“ (Kopieren), um die neue SNN in die Windows-Zwischenablage zu kopieren.
8. Öffnen Sie die Registerkarte „General“ (Allgemein) des Dialogfelds „Module Properties“ (Moduleigenschaften) des nächsten Sicherheits-E/A-Geräts unter diesem EtherNet/IP-Modul.
9. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.
10. Wählen Sie „Time-based“ (Zeitbasiert) und klicken Sie auf „Paste“ (Einfügen), um die SNN dieses EtherNet/IP-Netzwerks in dieses Gerät einzufügen.
11. Klicken Sie auf „OK“.
12. Wiederholen Sie die Schritte 8 bis 10 für die verbleibenden Sicherheits-E/A-Geräte unter diesem EtherNet/IP-Kommunikationsmodul.
13. Wiederholen Sie die Schritte 2 bis 10 für alle verbleibenden Netzwerkkommunikationsmodule im E/A-Konfigurationsbaum.

Kopieren und Einfügen einer Sicherheitsnetzwerknummer (SNN)

Falls eine andere Steuerung die Konfiguration eines Moduls verwaltet, können Sie die SNN aus der diese Konfiguration verwaltenden Steuerung kopieren und in das Modul in Ihrem E/A-Konfigurationsverzeichnis einfügen.

1. Öffnen Sie in der die Konfiguration verwaltenden Steuerung des Moduls über das Software-Konfigurationswerkzeug das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) für das Modul.



2. Klicken Sie auf „Copy“ (Kopieren).
3. Klicken Sie auf die Registerkarte „General“ (Allgemein) im Dialogfeld „Module Properties“ (Moduleigenschaften) des E/A-Geräts im E/A-Konfigurationsverzeichnis des konsumierenden Steuerungsprojekts.
   Diese konsumierende Steuerung ist nicht die die Konfiguration verwaltende Steuerung.

4. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.
5. Klicken Sie auf „Paste“ (Einfügen).
6. Klicken Sie auf „OK“.

EtherNet/IP-Kommunikation

Für die EtherNet/IP-Netzwerkkommunikation in einem GuardLogix-System stehen mehrere Module zur Auswahl. Für CIP Safety-Kommunikation, einschließlich Sicherheits-E/A-Gerätesteuerung, wählen Sie eines der in Tabelle 12 aufgeführten Module aus, mit Ausnahme des Moduls 1756-EWEB, das CIP Safety-Kommunikation nicht unterstützt.

Tabelle 12 enthält eine Auflistung der Module und ihrer primären Leistungsmerkmale.

Tabelle 12 – EtherNet/IP-Kommunikationsmodule und ihre Leistungsmerkmale

Modul	Leistungsmerkmale
1756-ENBT	• Anschluss von Steuerungen an E/A-Geräte (erfordert einen Adapter für verteilte E/A). • Kommunikation mit anderen EtherNet/IP-Geräten (Nachrichten). • Dient als Übertragungspfad für die gemeinsame Nutzung von Daten zwischen Logix5000-Steuerungen (Produzieren/Konsumieren). • Überbrückung von EtherNet/IP-Netzknoten zur Weiterleitung von Nachrichten an Geräte in anderen Netzwerken.
1756-EN2T	• Ausführung derselben Funktionen wie das Modul 1756-ENBT mit der doppelten Kapazität für anspruchsvollere Anwendungen. • Bereitstellung einer vorübergehenden Konfigurationsverbindung über den USB-Anschluss. • Schnelles Konfigurieren der IP-Adressen mithilfe von Drehschaltern.
1756-EN2F	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Anschließen von Glasfasermedien über einen LWL-Anschluss am Modul.
1756-EN2TXT	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Betrieb unter extremen Umgebungsbedingungen bei Temperaturen von –25 bis +70 °C.
1756-EN2TR	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Unterstützung der Kommunikation in einer Ringtopologie für ein DLR-Ringnetzwerk (Device Level Ring) mit Einzelfehlertoleranz.
1756-EN2TRXT	• Ausführen derselben Funktionen wie das Modul 1756-EN2T. • Unterstützung der Kommunikation in einer Ringtopologie für ein DLR-Ringnetzwerk (Device Level Ring) mit Einzelfehlertoleranz. • Betrieb unter extremen Umgebungsbedingungen bei Temperaturen von –25 bis +70 °C.
1756-EN3TR	• Ausführen derselben Funktionen wie das Modul 1756-EN2TR. • Zwei Anschlüsse für DLR-Verbindung.
1756-EWEB	• Bereitstellung anpassbarer Webseiten für den externen Zugriff auf Steuerungsinformationen. • Bereitstellung von dezentralem Zugriff über einen Internet-Browser auf Tags in einer lokalen ControlLogix-Steuerung. • Kommunikation mit anderen EtherNet/IP-Geräten (Nachrichten). • Überbrückung von EtherNet/IP-Netzknoten zur Weiterleitung von Nachrichten an Geräte in anderen Netzwerken. • Unterstützung von Ethernet-Geräten, die nicht auf EtherNet/IP mit einer Socket-Schnittstelle basieren. Dieses Modul bietet keine Unterstützung für E/A oder produzierte/konsumierte Tags und unterstützt auch nicht die CIP Safety-Kommunikation.

EtherNet/IP-Kommunikationsmodule bieten folgende Leistungsmerkmale:

- Unterstützung von Messaging, produzierten/konsumierten Tags, Bedienerschnittstellen und verteilten E/A
- Möglichkeit zur Verkapselung von Nachrichten im TCP/UDP/IP-Standardprotokoll
- Eine gemeinsame Applikationsebene mit ControlNet- und DeviceNet-Netzwerken
- Netzwerkverbindungen über ein RJ45-Kabel, Kategorie 5, nicht abgeschirmtes Twisted-Pair-Kabel
- Unterstützung von Halb-/Vollduplexbetrieb mit 10 Mbit/s oder 100 Mbit/s
- Unterstützung von Standard-Switches
- Keine Netzwerkplanung erforderlich
- Keine Routing-Tabellen erforderlich

Diese Softwareprodukte stehen für EtherNet/IP-Netzwerke zur Verfügung.

Tabelle 13 – Software für EtherNet/IP-Module

Software	Verwendungszweck	Erforderlich
Studio 5000-Umgebung	• Konfigurieren des Steuerungsprojekts • Definieren der EtherNet/IP-Kommunikation	Ja
Dienstprogramm BOOTP/DHCP(1)	Zuordnen von IP-Adressen zu Geräten in einem EtherNet/IP-Netzwerk	Nein
Software RSNetWorx™ for EtherNet/IP	Konfigurieren von EtherNet/IP-Geräten mithilfe von IP-Adressen und/oder Hostnamen	Nein
Software RSLinx	• Konfigurieren von Geräten • Einrichten der Kommunikation zwischen Geräten • Bereitstellen von Diagnosefunktionen	Ja

(1) Im Lieferumfang dieses Dienstprogramms ist die Studio 5000-Umgebung enthalten.

Produzieren und Konsumieren von Daten über ein EtherNet/IP-Netzwerk

Die Steuerung unterstützt die Möglichkeit, Tags über ein EtherNet/IP-Netzwerk zu produzieren (senden) und zu konsumieren (empfangen). Alle produzierten und konsumierten Tags benötigen eine Verbindung. Die Gesamtzahl der Tags, die produziert oder konsumiert werden kann, ist auf die Anzahl der verfügbaren Verbindungen beschränkt.

Verbindungen über das EtherNet/IP-Netzwerk

Sie bestimmen indirekt, wie viele Verbindungen die Sicherheitssteuerung verwendet, indem Sie die Steuerung so konfigurieren, dass sie mit anderen Geräten im System kommunizieren kann. Verbindungen sind Ressourcenzuordnungen, die im Vergleich zu nicht verbundenen Nachrichten (Nachrichtenbefehle) eine zuverlässigere Kommunikation zwischen Geräten ermöglichen.

EtherNet/IP-Verbindungen sind azyklisch. Eine azyklische Verbindung wird durch das angeforderte Paketintervall (RPI) für die E/A-Steuerung oder das Programm getriggert (z. B. ein MSG-Befehl). Azyklische Nachrichten ermöglichen Ihnen bei Bedarf das Senden und Empfangen von Daten.

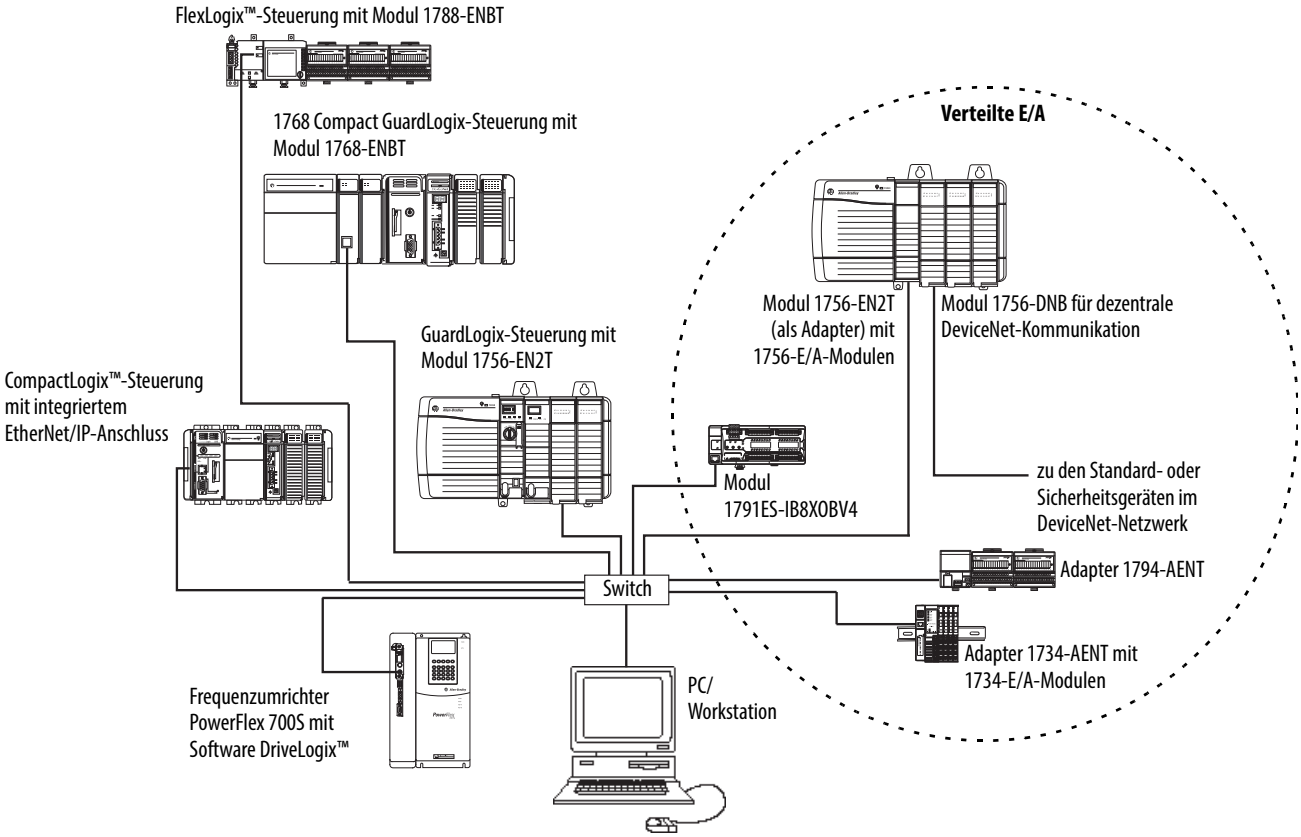
Die EtherNet/IP-Kommunikationsmodule unterstützen 128 CIP-Verbindungen (Common Industrial Protocol) über ein EtherNet/IP-Netzwerk.

Beispiele für die EtherNet/IP-Kommunikation

Abbildung 13 zeigt die folgenden Kommunikationsfunktionen:

- Die Steuerungen können Standard- oder Sicherheits-Tags untereinander produzieren und konsumieren.
- Die Steuerungen können MSG-Befehle initiieren, die Standarddaten senden/empfangen oder Geräte konfigurieren.(1)
- Das EtherNet/IP-Kommunikationsmodul wird als Bridge verwendet und lässt die Sicherheitssteuerung Standard- und Sicherheitsdaten produzieren und konsumieren.
- Die Workstation kann Projekte für die Steuerungen hoch- und herunterladen.
- Die Workstation kann Geräte im EtherNet/IP-Netzwerk konfigurieren.

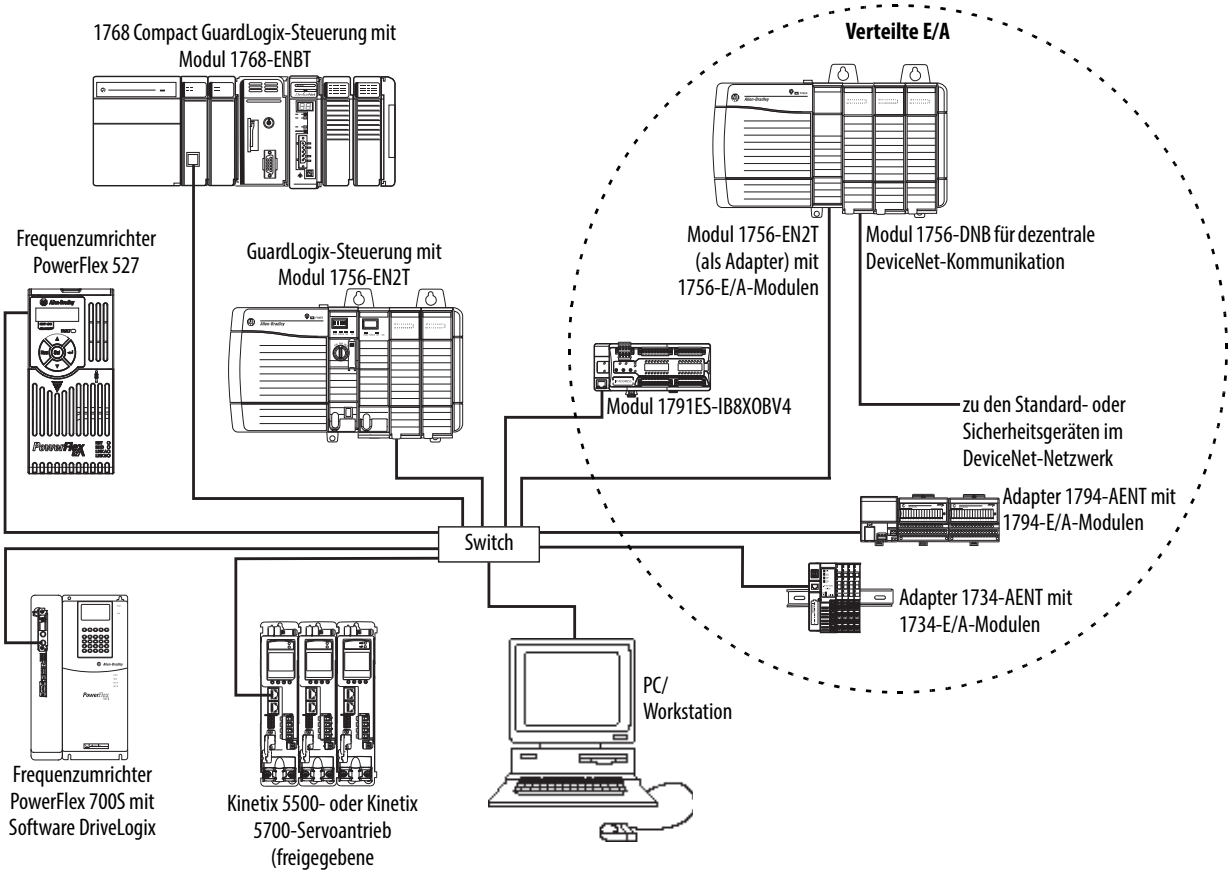
Abbildung 13 – Beispiel für die EtherNet/IP-Kommunikation



(1) GuardLogix-Steuerungen unterstützen keine MSG-Befehle für Sicherheitsdaten.

In der Anwendung Logix Designer, Version 24 und höher, werden sowohl die Standard- als auch die Sicherheitssteuerung über einen einzelnen Anschluss unterstützt.

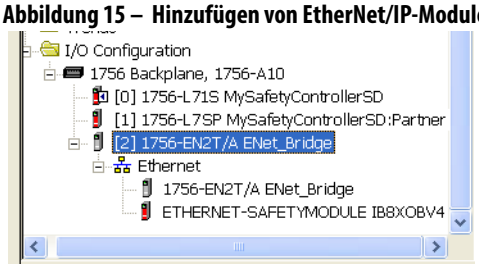
Abbildung 14 – Beispiel für EtherNet/IP-Kommunikation mit Standard- und Sicherheitsverbindung



EtherNet/IP-Verbindungen für Sicherheits-E/A-Geräte

Sicherheits-E/A-Geräte in EtherNet/IP-Netzwerken werden dem Projekt unter dem EtherNet/IP-Kommunikationsmodul hinzugefügt, wie unter Hinzufügen von Sicherheits-E/A-Geräten auf Seite 67 beschrieben. Wenn Sie ein Sicherheits-E/A-Gerät einfügen, erstellt die Anwendung Logix Designer für dieses Gerät automatisch Sicherheitsdaten-Tags im Steuerungsbereich.

Abbildung 15 – Hinzufügen von EtherNet/IP-Modulen zum Projekt



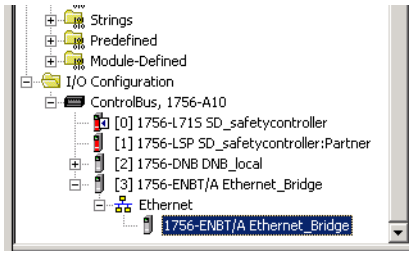
EtherNet/IP-Standardverbindungen

Wenn Sie ein Standard-EtherNet/IP-Modul mit der Sicherheitssteuerung verwenden möchten, fügen Sie das Modul dem Sicherheitssteuerungsprojekt hinzu und laden Sie das Projekt in die GuardLogix-Steuerung.

1. Definieren Sie zum Konfigurieren des Moduls die IP-Adresse, Subnet-Maske und den Gateway.

EtherNet/ IP-Parameter	Beschreibung
IP-Adresse	Die IP-Adresse kennzeichnet das Modul auf eindeutige Weise. Die IP-Adresse hat das Format *xxx.xxx.xxx.xxx*. Dabei steht die Zeichenfolge xxx jeweils für eine Zahl zwischen 0 und 255. Allerdings dürfen einige Werte nicht als erstes Oktett in der Adresse verwendet werden: • 000.*xxx.xxx.xxx* • 127.*xxx.xxx.xxx* • 223…255.*xxx.xxx.xxx*
Subnetz-Maske	Die Subnetz-Adressierung stellt eine Erweiterung des IP-Adressenschemas dar, durch das die Verwendung einer Netzwerk-ID für mehrere physische Netzwerke ermöglicht wird. Das Routing außerhalb des Standorts wird fortgesetzt, indem die IP-Adresse über die Klasse in eine Netz-ID und eine Host-ID aufgeteilt wird. Innerhalb eines Standorts wird die Subnet-Maske verwendet, um die IP-Adresse erneut in eine spezifische Netz-ID und eine Host-ID aufzuteilen. Dieses Feld wird standardmäßig auf den Wert 0.0.0.0 eingestellt. Falls Sie die Subnet-Maske eines bereits konfigurierten Moduls ändern, müssen Sie dieses aus- und wiedereinschalten, damit die Änderung wirksam wird.
Gateway	Ein Gateway verbindet individuelle physische Netzwerke zu einem System von Netzwerken. Wenn ein Netzknoten mit dem Netzknoten eines anderen Netzwerks kommunizieren muss, überträgt ein Gateway die Daten zwischen den beiden Netzwerken. Dieses Feld wird standardmäßig auf den Wert 0.0.0.0 eingestellt.

2. Nachdem Sie das EtherNet/IP-Modul physisch installiert und seine IP-Adresse festgelegt haben, müssen Sie das Modul dem Controller Organizer (Steuerungsorganisator) Ihres GuardLogix-Steuerungsprojekts hinzufügen.



3. Verwenden Sie die Anwendung Logix Designer, um das Projekt herunterzuladen.

ControlNet-Kommunikation

Wählen Sie für die ControlNet-Kommunikation das Modul 1756-CNB oder 1756-CNBR für die Standardkommunikation oder das Modul 1756-CN2, 1756-CN2R oder 1756-CN2RXT für die Sicherheitskommunikation.

Tabelle 14 – ControlNet-Module

Wenn Ihre Anwendung	Wählen Sie
• Standard-E/A-Geräte steuert • einen Adapter für verteilte E/A auf ControlNet-Verbindungen benötigt • mit anderen ControlNet-Geräten kommuniziert (Nachrichten) • Standarddaten gemeinsam mit anderen Logix5000-Steuerungen verwendet (produziert/konsumiert) • ControlNet-Verbindungen überbrückt, um Nachrichten an Geräte in anderen Netzwerken weiterzuleiten	1756-CNB
• dieselben Funktionen ausführt wie das Modul 1756-CNB • auch redundant ausgelegte ControlNet-Medien unterstützt	1756-CNBR
• dieselben Funktionen ausführt, die vom Modul 1756-CNB mit höherer Leistung unterstützt werden • die CIP Safety-Kommunikation unterstützt	1756-CN2
• dieselben Funktionen ausführt wie das Modul 1756-CN2 • auch redundant ausgelegte ControlNet-Medien unterstützt	1756-CN2R
• dieselben Funktionen ausführt wie das Modul 1756-CN2R • unter extremen Umgebungsbedingungen bei Temperaturen zwischen –25 bis +70 °C betrieben wird	1756-CN2RXT

Diese Softwareprodukte stehen für ControlNet-Netzwerke zur Verfügung.

Tabelle 15 – Software für ControlNet-Module

Software	Verwendungszweck	Erforderlich
Studio 5000-Umgebung	• Konfigurieren von GuardLogix-Projekten • Definieren der ControlNet-Kommunikation	Ja
Software RSNetWorx for ControlNet	• Konfigurieren des ControlNet-Netzwerks • Definieren der Netzwerkaktualisierungszeit (NUT) • Planen des ControlNet-Netzwerks	Ja
Software RSLinx	• Konfigurieren von Geräten • Einrichten der Kommunikation zwischen Geräten • Bereitstellen von Diagnosefunktionen	Ja

Das ControlNet-Kommunikationsmodul bietet folgende Leistungsmerkmale:

- Es unterstützt das Messaging, produzierte/konsumierte Sicherheits- und Standard-Tags sowie verteilte E/A.
- Es unterstützt die Verwendung von Koax- und Glasfaser-Repeatern zur Isolierung und bei größeren Entfernungen.

Produzieren und Konsumieren von Daten über ein ControlNet-Netzwerk

Die GuardLogix-Steuerung unterstützt die Möglichkeit, Tags über ControlNet-Netzwerke zu produzieren (senden) und zu konsumieren (empfangen). Die Gesamtzahl der Tags, die produziert oder konsumiert werden kann, ist auf die Anzahl der verfügbaren Verbindungen in der GuardLogix-Steuerung beschränkt.

Verbindungen über das ControlNet-Netzwerk

Die Anzahl der von der Steuerung verwendeten Verbindungen wird dadurch bestimmt, wie Sie die Steuerung zum Kommunizieren mit anderen Geräten im System verwenden. Verbindungen sind Ressourcenzuordnungen, die im Vergleich zu nicht verbundenen Nachrichten eine zuverlässigere Kommunikation zwischen Geräten ermöglichen.

ControlNet-Verbindungen können zyklisch oder azyklisch sein.

Tabelle 16 – ControlNet-Verbindungen

Verbindungstyp	Beschreibung
Zyklisch (nur beim ControlNet-Netzwerk)	Eine zyklische Verbindung gibt es nur bei der ControlNet-Kommunikation. Eine zyklische Verbindung ermöglicht Ihnen das wiederholte Senden und Empfangen von Daten mit einem vordefinierten Intervall, dem angeforderten Paketintervall (RPI). Beispielsweise ist eine Verbindung zu einem E/A-Gerät eine zyklische Verbindung, da Sie Daten von dem Modul wiederholt und mit einem festgelegten Intervall empfangen können. Weitere zyklische Verbindungen umfassen Verbindungen zu: • Kommunikationsgeräten • produzierten/konsumierten Tags In einem ControlNet-Netzwerk müssen Sie die Software RSNetWorx for ControlNet verwenden, um zyklische Verbindungen zu aktivieren und eine Netzwerkaktualisierungszeit (NUT) festzulegen. Beim Planen einer Verbindung wird Netzwerkbandbreite speziell für diese Verbindung reserviert.
Azyklisch	Eine azyklische Verbindung (unscheduled connection) ist eine Nachrichtenübertragung zwischen Steuerungen, die vom angeforderten Paketintervall (RPI) oder vom Programm getriggert wird (z. B. ein MSG-Befehl). Azyklische Nachrichten ermöglichen Ihnen bei Bedarf das Senden und Empfangen von Daten. Azyklische Verbindungen verwenden die Netzwerkbandbreite, die verbleibt, nachdem zyklische Verbindungen zugeordnet wurden. Produzierte/konsumierte Sicherheitsverbindungen sind azyklisch.

Die Kommunikationsmodule 1756-CNB und 1756-CNBR unterstützen 64 CIP-Verbindungen über ein ControlNet-Netzwerk. Für eine optimale Leistung sollten Sie jedoch maximal 48 Verbindungen pro Modul konfigurieren.

Das Modul 1756-CN2 unterstützt 128 CIP-Verbindungen über das ControlNet-Netzwerk.

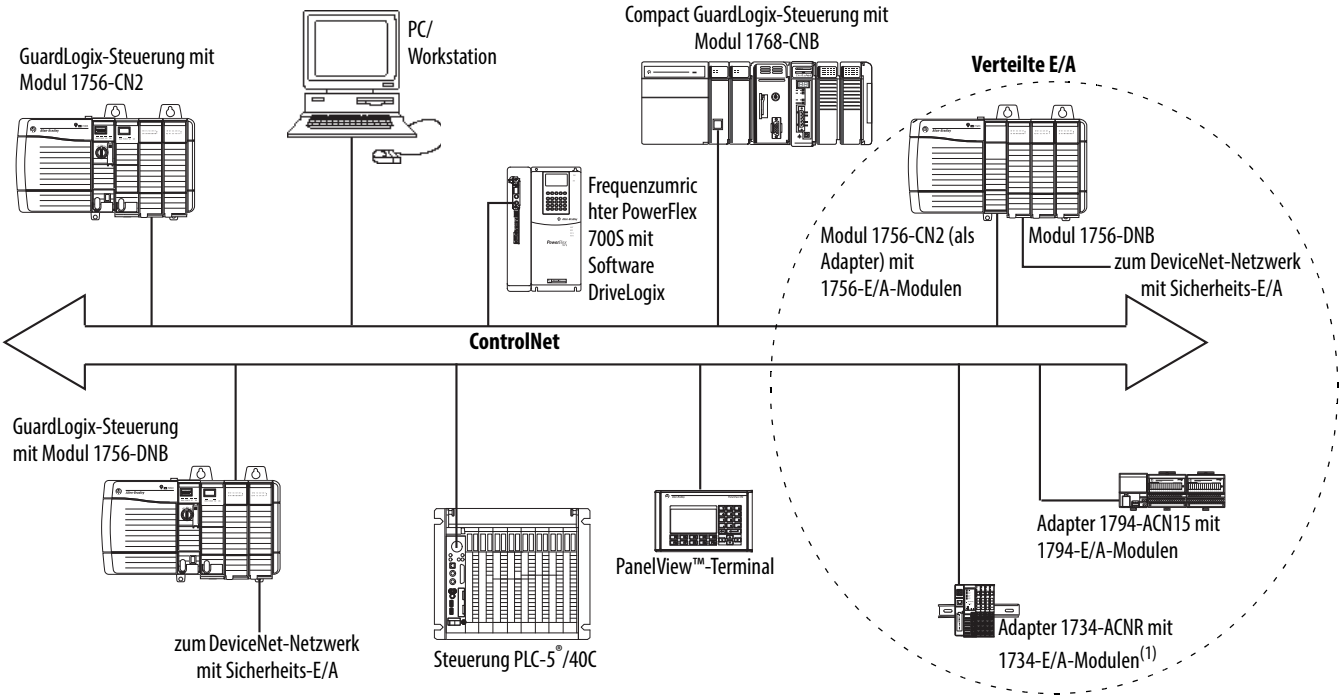
Beispiel für die ControlNet-Kommunikation

In diesem Beispiel:

- können GuardLogix-Steuerungen Standard- oder Sicherheits-Tags untereinander produzieren und konsumieren.
- GuardLogix können Steuerungen MSG-Befehle initiieren, die Standarddaten senden/empfangen oder Geräte konfigurieren.(1)
- kann das Modul 1756-CN2 als Bridge verwendet werden, wodurch die GuardLogix-Steuerung Standard- und Sicherheitsdaten von den E/A-Geräten konsumieren und für diese produzieren kann.
- kann der PC Projekte von den Steuerungen hochladen oder auf diese herunterladen.
- kann der PC Geräte im ControlNet-Netzwerk und das Netzwerk selbst konfigurieren.

(1) unterstützen die GuardLogix-Steuerungen keine MSG-Befehle für Sicherheitsdaten.

Abbildung 16 – Beispiel für die ControlNet-Kommunikation



(1) Der Adapter 1734-ACN unterstützt keine POINT Guard-Sicherheits-E/A-Module.

ControlNet-Verbindungen für dezentrale E/A

Fügen Sie für die Kommunikation mit dezentralen E/A-Geräten über ein ControlNet-Netzwerk im Ordner „I/O Configuration“ (E/A-Konfiguration) eine ControlNet-Bridge, einen ControlNet-Adapter sowie E/A-Geräte ein.

DeviceNet-Kommunikation

Für die Kommunikation und den Datenaustausch mit Sicherheits-E/A-Geräten in DeviceNet-Netzwerken benötigen Sie das Modul 1756-DNB im lokalen Chassis.

Informationen zum Installieren des Moduls 1756-DNB finden Sie in der Publikation 1756-IN566, ControlLogix DeviceNet Scanner Module Installation Instructions.

Das Modul 1756-DNB unterstützt die Kommunikation mit den DeviceNet-Safety-Geräten und den DeviceNet-Standardgeräten. Sie können beide Typen verwenden.

Die folgenden Softwareprodukte stehen für DeviceNet-Netzwerke und das Modul 1756-DNB zur Verfügung.

Tabelle 17 – Software für DeviceNet-Netzwerke

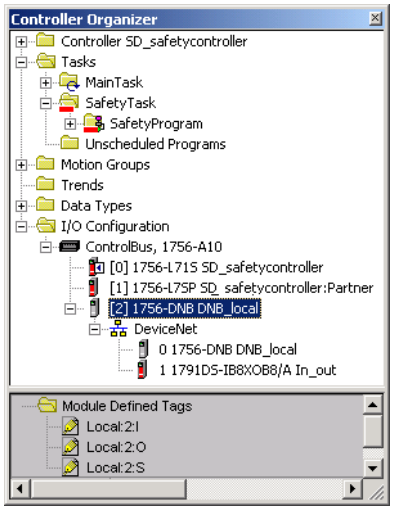
Software	Verwendungszweck	Erforderlich
Studio 5000-Umgebung	• Konfigurieren von ControlLogix-Projekten. • Definieren der DeviceNet-Kommunikation.	Ja
Software RSNetWorx for DeviceNet	• Konfigurieren von DeviceNet-Geräten. • Definieren der Abtastliste für diese Geräte.	Ja
Software RSLinx Classic oder RSLinx Enterprise	• Konfigurieren von Kommunikationsgeräten. • Bereitstellen von Diagnosefunktionen. • Einrichten der Kommunikation zwischen Geräten.	Ja

DeviceNet-Verbindungen für Sicherheits-E/A-Geräte

Zugriff auf Sicherheits-E/A-Geräte in DeviceNet-Netzwerken erhalten Sie, indem Sie das Modul 1756-DNB dem E/A-Konfigurationsbaum des GuardLogix-Steuerungsprojekts hinzufügen.

Sicherheits-E/A-Geräte in DeviceNet-Netzwerken werden dem Projekt unter dem Modul 1756-DNB hinzugefügt, wie in Kapitel 5, Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen, beschrieben. Wenn Sie ein Sicherheits-E/A-Gerät einfügen, erstellt die Anwendung Logix Designer für dieses Gerät automatisch Sicherheitsdaten-Tags im Steuerungsbereich.

Abbildung 17 – DeviceNet-Modul in der Steuerung im E/A-Konfigurationsverzeichnis



Standard-DeviceNet-Verbindungen

Falls Sie Standard-DeviceNet-E/A mit Ihrer GuardLogix-Steuerung verwenden, müssen Sie jedem 1756-DNB-Modul zwei Verbindungen zuweisen. Eine Verbindung ist für den Modulstatus und die Konfiguration bestimmt. Die andere Verbindung ist eine Rack-optimierte Verbindung für die DeviceNet-E/A-Daten.

Wenn Sie das Modul 1756-DNB für den Zugriff auf Standarddaten über das DeviceNet-Netzwerk nutzen möchten, müssen Sie die Software RSNetWorx for DeviceNet verwenden, um:

- eine Konfigurationsdatei für das Netzwerk zu erstellen.
- jedes Standardgerät im Netzwerk zu konfigurieren.
- das Modul 1756-DNB zu konfigurieren.
- die Standard-E/A-Geräte in die 1756-DNB-Abtastliste einzufügen.

Wenn Sie das Modul 1756-DNB zur E/A-Konfiguration der Steuerung hinzufügen, erstellt die Anwendung Logix Designer automatisch einen Satz Standard-Tags für die Eingangs-, Ausgangs- und Zustandsdaten des Netzwerks.

Hinzufügen, Konfigurieren, Überwachen und Ersetzen von CIP Safety-E/A-Modulen

Thema	Seite
Hinzufügen von Sicherheits-E/A-Geräten	67
Konfigurieren von Sicherheits-E/A-Geräten	68
Festlegen der IP-Adresse mit Network Address Translation (NAT)	69
Festlegen der Sicherheitsnetzwerknummer (SNN)	71
Verwenden von Unicast-Verbindungen auf EtherNet/IP-Netzwerken	71
Festlegen der Reaktionszeitgrenze der Verbindung	71
Verstehen der Konfigurationssignatur	75
Zurücksetzen der Verwaltungsrechte an Sicherheits-E/A-Geräten	76
Adressieren von Sicherheits-E/A-Daten	77
Überwachen des Sicherheits-E/A-Gerätestatus	79
Zurücksetzen eines Moduls auf die Werkseinstellungen	80
Austauschen eines Geräts über die Anwendung Logix Designer	81
Austauschen eines POINT Guard I/O-Moduls über die Software RSNetWorx for DeviceNet	87

Weitere Informationen zu Installation, Konfiguration und Betrieb der Sicherheits-E/A-Geräte finden Sie unter Weitere Informationen auf Seite 14.

Hinzufügen von Sicherheits-E/A-Geräten

Wenn Sie ein Sicherheits-E/A-Gerät in das System einfügen, müssen Sie eine Konfiguration für das Gerät definieren, zu der unter anderem Folgendes gehört:

- Netzknotenadresse für DeviceNet-Netzwerke

  Die Netzknotenadresse eines Sicherheits-E/A-Geräts in DeviceNet-Netzwerken kann nicht über die Anwendung Logix Designer festgelegt werden. Knotenadressen werden über Drehschalter an den Geräten festgelegt.

- IP-Adresse für EtherNet/IP-Netzwerke

  Zum Festlegen der IP-Adresse können Sie die Drehschalter am Modul entsprechend anpassen, die DHCP-Software verwenden, die Sie von Rockwell Automation erhalten, die Anwendung Logix Designer verwenden oder die Standardadresse aus dem nichtflüchtigen Speicher abrufen.

- Sicherheitsnetzwerknummer (SNN – Safety Network Number)

  Informationen zum Festlegen der SNN finden Sie auf Seite 71.

- Konfigurationssignatur

  Informationen darüber, wann die Konfigurationssignatur automatisch festgelegt wird und wann Sie die Signatur festlegen müssen, finden Sie auf Seite 75.
- Reaktionszeitgrenze

  Informationen zum Festlegen des Grenzwerts für die Reaktionszeit finden Sie auf Seite 71.
- Sicherheitseingangs-, Sicherheitsausgangs- und Testparameter schließen die Modulkonfiguration ab.

Sie können Sicherheits-E/A-Geräte über die GuardLogix-Steuerung mithilfe der Anwendung Logix Designer konfigurieren.

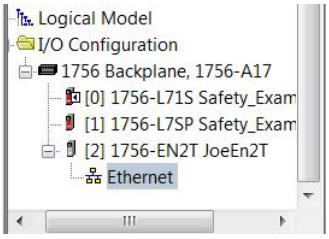
HINWEIS Sicherheits-E/A-Geräte unterstützen Standard- und Sicherheitsdaten. Die Gerätekonfiguration definiert, welche Daten zur Verfügung stehen.

Konfigurieren von Sicherheits-E/A-Geräten

Fügen Sie dem Kommunikationsmodul das Sicherheits-E/A-Gerät unter dem Ordner „I/O Configuration“ (E/A-Konfiguration) des Steuerungsprojekts hinzu.

HINWEIS Sie können ein Sicherheits-E/A-Gerät weder hinzufügen noch löschen, solange Sie sich im Online-Modus befinden.

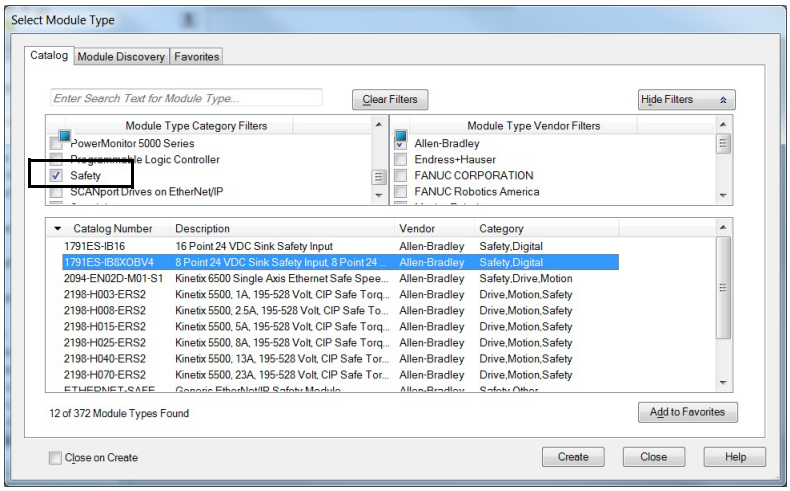
1. Klicken Sie mit der rechten Maustaste auf das DeviceNet- oder Ethernet-Netzwerk und wählen Sie „New Module“ (Neues Modul) aus.



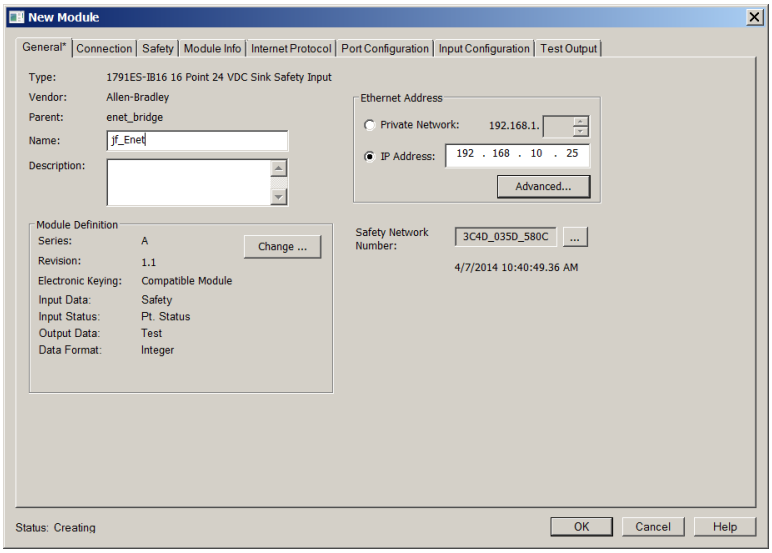
In diesem Beispiel wird ein Ethernet-Netzwerk verwendet.

2. Wählen Sie auf der Registerkarte „Catalog“ (Katalog) das Sicherheits-E/A-Gerät aus.

HINWEIS Verwenden Sie die Filter, um die Liste der Module in der Auswahl zu reduzieren.



3. Klicken Sie auf „Create“ (Erstellen).
4. Geben Sie einen Namen für das neue Gerät ein.



5. Ändern Sie die Einstellungen unter „Module Definition“ (Moduldefinition), falls erforderlich, indem Sie auf „Change“ (Ändern) klicken.
6. Geben Sie die Knotenadresse für DeviceNet-Netzwerke oder die IP-Adresse für EtherNet/IP-Netzwerke ein.

   Das Pulldown-Menü enthält nur freie Netzknotennummern.

   Wenn Ihr Netzwerk die Network Address Translation (NAT) verwendet, siehe Festlegen der IP-Adresse mit Network Address Translation (NAT) auf Seite 69.
7. Um die Sicherheitsnetzwerknummer zu ändern, klicken Sie auf die Schaltfläche ... (falls erforderlich).

   Ausführliche Informationen hierzu finden Sie auf Seite 71.
8. Legen Sie die Reaktionszeitgrenze der Verbindung mithilfe der Registerkarte „Safety“ (Sicherheit) fest.

   Ausführliche Informationen hierzu finden Sie auf Seite 71.
9. Informationen zur Konfiguration des Sicherheits-E/A-Geräts finden Sie in der zugehörigen Benutzerdokumentation und in der Online-Hilfe der Anwendung Logix Designer.

Festlegen der IP-Adresse mit Network Address Translation (NAT)

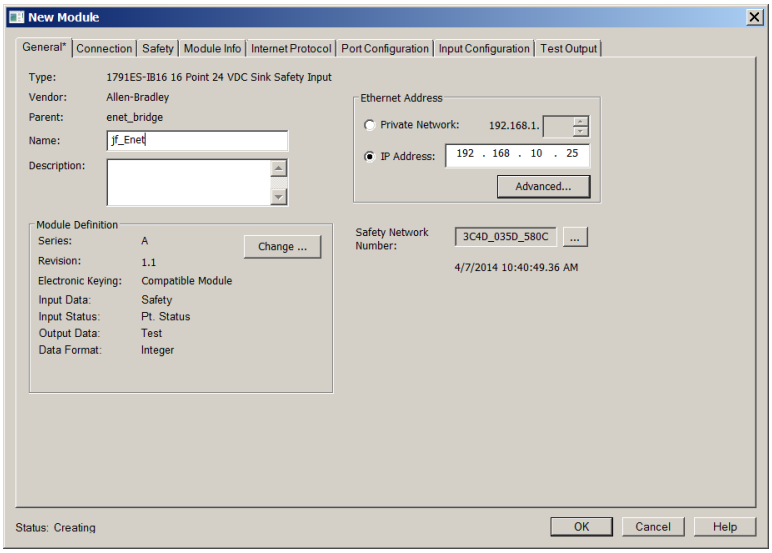
NAT übersetzt eine IP-Adresse über einen NAT-konfigurierten Router oder Switch in eine andere IP-Adresse. Der Switch übersetzt die Quell- und Zieladresse innerhalb von Datenpaketen während des Datenverkehrs zwischen Subnetzen.

Dieser Dienst ist nützlich, wenn Sie IP-Adressen in einem Netzwerk wiederverwenden müssen. Durch NAT können Geräte in mehrere identische private Subnetze segmentiert werden und gleichzeitig eindeutige Identitäten im öffentlichen Subnetz behalten.

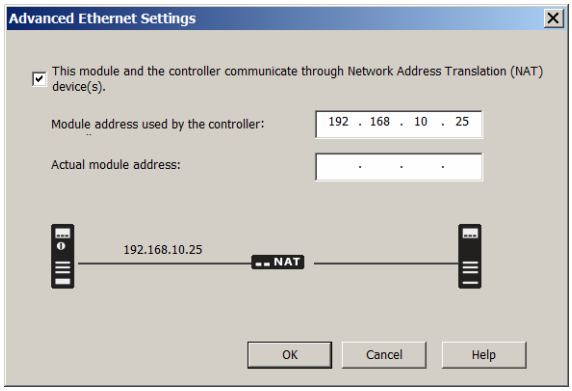
Bei Verwendung von NAT gehen Sie wie folgt vor, um die IP-Adresse einzurichten.

1. Geben Sie im Feld „IP Address“ die IP-Adresse ein, die die Steuerung verwenden soll.

   Dies ist in der Regel bei der Verwendung von NAT die IP-Adresse im öffentlichen Netzwerk.



2. Klicken Sie auf „Advanced“ (Erweitert), um das Dialogfeld „Advanced Ethernet Settings“ (Erweiterte Ethernet-Einstellungen) zu öffnen.



3. Aktivieren Sie das Kontrollkästchen, um anzugeben, dass dieses Modul und die Steuerung über NAT-Geräte kommunizieren.
4. Geben Sie die tatsächliche Moduladresse ein.

HINWEIS Wenn Sie die IP-Adresse mithilfe der Drehschalter konfiguriert haben, handelt es sich um die Adresse, die Sie für das Gerät festlegen. Die tatsächliche Moduladresse ist dieselbe Adresse, die auf der Registerkarte „Internet Protocol“ des Geräts angezeigt wird.

5. Klicken Sie auf „OK“.

Die Steuerung verwendet die übersetzte Adresse, das CIP Safety-Protokoll benötigt jedoch die tatsächliche Adresse des Geräts.

Festlegen der Sicherheitsnetzwerknummer (SNN)

Die Zuordnung einer zeitbasierten SNN erfolgt automatisch, wenn neue Sicherheits-E/A-Geräte hinzugefügt werden. Werden zu einem späteren Zeitpunkt Sicherheitsgeräte zum gleichen Netzwerk hinzugefügt, wird ihnen die gleiche SNN zugeordnet, die innerhalb der niedrigsten Adresse auf diesem CIP Safety-Netzwerk definiert ist.

Für die meisten Anwendungen ist diese automatische, zeitbasierte SNN ausreichend. Es gibt jedoch Fälle, in denen eine Änderung der SNNs erforderlich ist.

Siehe Zuordnen der Sicherheitsnetzwerknummer (SNN) auf Seite 53.

Verwenden von Unicast-Verbindungen auf EtherNet/IP-Netzwerken

Unicast-Verbindungen sind Punkt-zu-Punkt-Verbindungen zwischen einem Quell- und einem Zielknoten. Für diese Verbindungsart müssen Sie keinen minimalen oder maximalen RPI-Grenzwert oder Standardwert festlegen.

Wählen Sie zur Konfiguration von Unicast-Verbindungen die Registerkarte „Connection“ (Verbindung) und anschließend „Use Unicast Connection over Ethernet/IP“ (Unicast-Verbindung über EtherNet/IP verwenden) aus.

Festlegen der Reaktionszeitgrenze der Verbindung

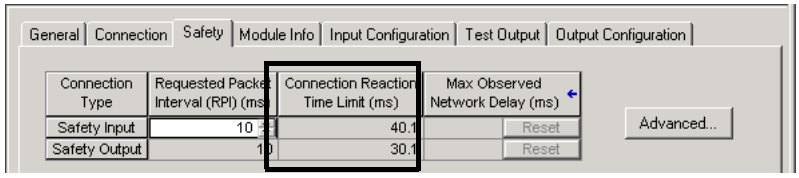
Die Reaktionszeitgrenze der Verbindung ist das maximale Alter der Sicherheitspakete auf der zugehörigen Verbindung. Falls das Alter der vom konsumierenden Gerät verwendeten Daten die Reaktionszeitgrenze der Verbindung überschreitet, tritt ein Verbindungsfehler ein. Die Reaktionszeitgrenze der Verbindung wird durch die folgenden Gleichungen bestimmt:

Reaktionszeitgrenze der Eingangsverbindung =
Eingang RPI x [Timeout-Multiplikator + Netzwerkverzögerungs-Multiplikator]

Reaktionszeitgrenze der Ausgangsverbindung =
Zeitspanne der Sicherheits-Task x [Timeout-Multiplikator + Netzwerkverzögerungs-Multiplikator – 1]

Die Reaktionszeitgrenze der Verbindung ist auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) angegeben.

Abbildung 18 – Reaktionszeitgrenze der Verbindung



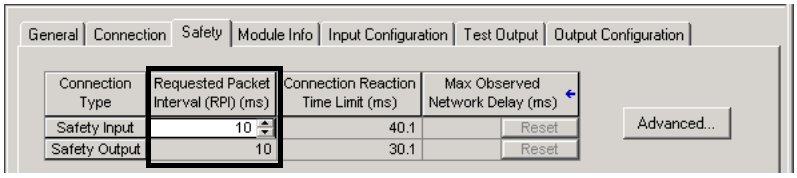
Spezifizieren des angeforderten Paketintervalls (RPI)

Das angeforderte Paketintervall (RPI) spezifiziert den Zeitraum, in dem die Daten über eine Verbindung aktualisiert werden. Ein Eingangsmodul erstellt beispielsweise Daten mit dem von Ihnen zugewiesenen RPI.

Für Sicherheits-Eingangsverbindungen können Sie das RPI auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) einstellen. Das angeforderte Paketintervall (RPI) wird in Schritten von 1 ms und innerhalb eines Bereichs von 1–100 ms eingegeben. Der Standardwert ist 10 ms.

Die Reaktionszeitgrenze der Verbindung wird sofort angepasst, wenn das RPI über die Anwendung Logix Designer geändert wird.

Abbildung 19 – Angefordertes Paketintervall (RPI)



Für Sicherheits-Ausgangsverbindungen wird das RPI anhand der Zeitspanne der Sicherheits-Task festgelegt. Falls eine entsprechende Reaktionszeitgrenze der Verbindung nicht zufriedenstellend ist, können Sie die Zeitspanne der Sicherheits-Task über das Dialogfeld „Safety Task Properties“ (Eigenschaften der Sicherheits-Task) anpassen.

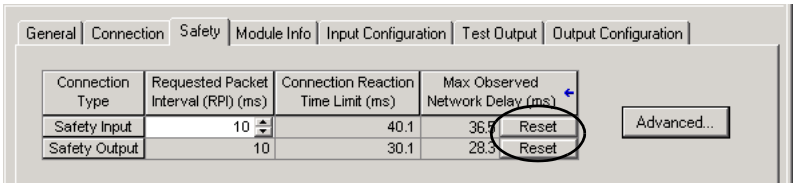
Unter Spezifizieren der Sicherheits-Task-Zeitspanne auf Seite 92 finden Sie weitere Informationen über die Zeitspanne der Sicherheits-Task.

Für die meisten Anwendungen ist das Standard-RPI in der Regel unzureichend. Für komplexere Anforderungen verwenden Sie die Schaltfläche „Advanced“ (Erweitert), um die Parameter der Reaktionszeitgrenze der Verbindung zu ändern, wie auf Seite 73 beschrieben.

Anzeigen der beobachteten maximalen Netzwerkverzögerung

Wenn die GuardLogix-Steuerung ein Sicherheitspaket empfängt, zeichnet die Software die beobachtete maximale Netzwerkverzögerung auf. Für Sicherheitseingänge zeigt die beobachtete maximale Netzwerkverzögerung die Verzögerung durch die Übertragung vom Eingangsmodul zur Steuerung und zurück sowie die Rückbestätigung zum Eingangsmodul an. Für Sicherheitsausgänge zeigt sie die Verzögerung durch die Übertragung von der Steuerung zum Ausgangsmodul und zurück sowie die Rückbestätigung zur Steuerung an. Die beobachtete maximale Netzwerkverzögerung wird auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) dargestellt. Wenn Sie online sind, klicken Sie auf „Reset“ (Zurücksetzen Max), um die beobachtete maximale Netzwerkverzögerung zurückzusetzen.

Abbildung 20 – Zurücksetzen der beobachteten maximalen Netzwerkverzögerung

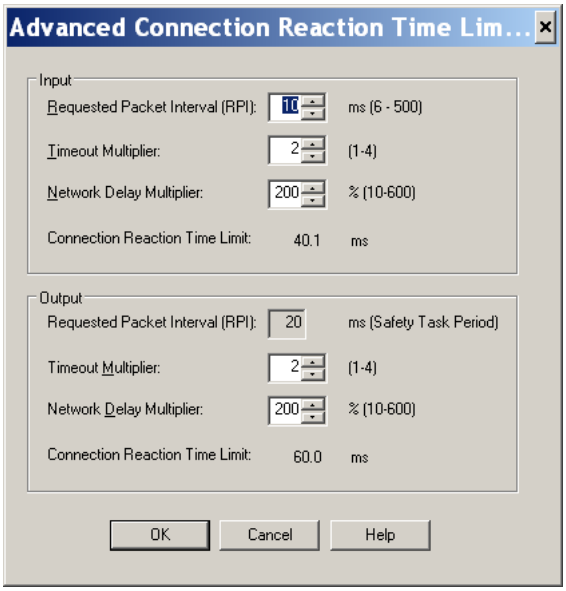


WICHTIG Die tatsächliche maximale Netzwerkverzögerungszeit vom Producer zum Consumer ist kürzer als der auf der Registerkarte „Safety" (Sicherheit) im Feld „Maximum Network Delay" (Maximale Netzwerkverzögerung) angezeigte Wert. Im Allgemeinen beträgt die tatsächliche maximale Nachrichtenverzögerung etwa die Hälfte des Werts der angezeigten maximalen Netzwerkverzögerung.

Festlegen der erweiterten Parameter für die Reaktionszeitgrenze der Verbindung

Konfigurieren Sie Verbindungsparameter wie Timeout-Multiplikator und Netzwerkverzögerungs-Multiplikator im Dialogfeld zum Festlegen der erweiterten Parameter für die Reaktionszeitgrenze der Verbindung.

Abbildung 21 – Erweiterte Konfiguration



Timeout-Multiplikator

Der Timeout-Multiplikator bestimmt die Anzahl der RPIs, die auf ein Paket gewartet wird, bevor ein Verbindungs-Timeout erfolgt. Dies lässt sich durch die Anzahl der Nachrichten ausdrücken, die verloren gehen können, bevor ein Verbindungsfehler ausgewiesen wird.

Ein Timeout-Multiplikator von 1 zeigt beispielsweise an, dass Nachrichten während jedes RPI-Intervalls empfangen werden müssen. Ein Timeout-Multiplikator von 2 zeigt an, dass 1 Nachricht verloren gehen kann, solange mindestens 1 Nachricht innerhalb eines zweimaligen RPI (2 x RPI) empfangen wird.

Netzwerkverzögerungs-Multiplikator

Der Netzwerkverzögerungs-Multiplikator definiert die Nachrichtentransportzeit, die durch das Sicherheitsprotokoll CIP Safety erzwungen wird. Der Netzwerkverzögerungs-Multiplikator spezifiziert die Verzögerung durch die Übertragung vom Producer zum Consumer und zurück und die Rückbestätigung zum Producer. Sie können den Netzwerkverzögerungs-Multiplikator verwenden, um die Reaktionszeitgrenze der Verbindung in solchen Fällen zu erhöhen oder zu verringern, in denen die erzwungene Nachrichtentransportzeit wesentlich geringer oder höher ist als das RPI. Das Einstellen des Netzwerkverzögerungs-Multiplikators kann beispielsweise hilfreich sein, wenn das RPI einer Ausgangsverbindung mit einer langen Sicherheits-Task-Zeitspanne übereinstimmt.

In Fällen, in denen das Eingangs-RPI oder das Ausgangs-RPI im Vergleich zur erzwungenen Nachrichtenverzögerungszeit relativ lang bzw. kurz ist, kann der Netzwerkverzögerungs-Multiplikator mithilfe einer der beiden Methoden angenähert werden.

Methode 1: Verwenden Sie das Verhältnis zwischen dem Eingangs-RPI und der Sicherheits-Task-Zeitspanne. Verwenden Sie diese Methode nur, wenn alle der nachfolgenden Bedingungen zutreffen:

- der Pfad oder die Verzögerung sind ungefähr identisch mit dem Ausgangspfad oder der Ausgangsverzögerung und
- das Eingangs-RPI wurde so konfiguriert, dass die tatsächliche Eingangsnachrichten-Transportzeit kürzer ist als das Eingangs-RPI und
- die Sicherheits-Task-Zeitspanne im Vergleich zum Eingangs-RPI lang ist.

  Unter diesen Bedingungen kann der Ausgangs-Netzwerkverzögerungs-Multiplikator wie folgt angenähert werden:

  Eingangs-Netzwerkverzögerungs-Multiplikator x [Eingangs-RPI ÷ Sicherheits-Task-Zeitspanne]

BEISPIEL **Berechnung des angenäherten Ausgangs-Netzwerkverzögerungs-Multiplikators**

Wenn:

Eingangs-RPI = 10 ms
Eingangs-Netzwerkverzögerungs-Multiplikator = 200 %
Sicherheits-Task-Zeitspanne = 20 ms

Dann ist der Ausgangs-Netzwerkverzögerungs-Multiplikator gleich:

200 % x [10 ÷ 20] = 100 %

Methode 2: Verwenden Sie die beobachtete maximale Netzwerkverzögerung. Wenn das System über einen längeren Zeitraum unter den ungünstigsten Belastungsbedingungen betrieben wird, kann der Netzwerkverzögerungs-Multiplikator ausgehend von der beobachteten maximalen Netzwerkverzögerung festgelegt werden. Dieses Verfahren kann bei einer Eingangs- oder Ausgangsverbindung angewendet werden. Protokollieren Sie die beobachtete maximale Netzwerkverzögerung, nachdem das System über einen längeren Zeitraum unter den ungünstigsten Belastungsbedingungen betrieben wurde.

Der Netzwerkverzögerungs-Multiplikator kann mit folgender Gleichung angenähert werden:

[Beobachtete maximale Netzwerkverzögerung + Toleranzfaktor] ÷ RPI

BEISPIEL **Berechnung des Netzwerkverzögerungs-Multiplikators aus der beobachteten maximalen Netzwerkverzögerung**

Wenn:

RPI = 50 ms
Beobachtete maximale Netzwerkverzögerung = 20 ms
Toleranzfaktor = 10

Dann ist der Netzwerkverzögerungs-Multiplikator gleich:

[20 + 10] ÷ 50 = 60 %

Tabelle 18 – Weitere Informationen

Quelle	Beschreibung
Steuerungssysteme GuardLogix 5570 – Sicherheitsreferenzhandbuch, Publikation 1756-RM099	Enthält Informationen zur Berechnung von Reaktionszeiten.
Guard I/O DeviceNet-Sicherheitsmodule – Benutzerhandbuch, Publikation 1791DS-UM001	
Guard I/O EtherNet/IP Safety Modules User Manual, Publikation 1791ES-UM001	

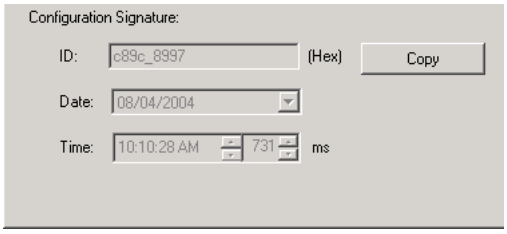
Verstehen der Konfigurationssignatur

Jedes Sicherheitsgerät hat eine eindeutige Konfigurationssignatur, die die Modulkonfiguration definiert. Die Konfigurationssignatur besteht aus einer Identifikationsnummer (ID-Nummer), Datum und Uhrzeit. Sie dient zur Verifizierung der Konfiguration eines Moduls.

Konfiguration über die Anwendung Logix Designer

Beim Konfigurieren des E/A-Geräts mithilfe der Anwendung Logix Designer wird die Konfigurationssignatur automatisch generiert. Sie können die Konfigurationssignatur über die Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Module Properties“ (Moduleigenschaften) einsehen und kopieren.

Abbildung 22 – Einsehen und Kopieren der Konfigurationssignatur



Anderer Konfigurationsverwalter (Listen-only-Verbindung)

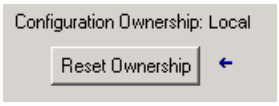
Wenn eine andere Steuerung die Verwaltungsrechte an der E/A-Gerätekonfiguration hat, müssen Sie die Signatur der Modulkonfiguration aus dem Projekt der über die Verwaltungsrechten verfügenden Steuerung kopieren und auf der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Module Properties“ (Moduleigenschaften) einfügen.

HINWEIS Falls das Gerät nur für Eingänge konfiguriert ist, können Sie die Konfigurationssignatur kopieren und einfügen. Verfügt das Gerät über Sicherheitsausgänge, wird es von der Steuerung verwaltet, die die Verwaltungsberechtigung für die Konfiguration hat. Das Textfeld mit der Konfigurationssignatur steht in diesem Fall nicht zur Verfügung.

Zurücksetzen der Verwaltungsrechte an Sicherheits-E/A-Geräten

Wenn das Steuerungsprojekt online geschaltet ist, zeigt die Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) die aktuellen Verwaltungsrechte an der Konfiguration an. Wenn das geöffnete Projekt die Verwaltungsberechtigung für die Konfiguration hat, wird „Local“ (Zentral) angezeigt. Wenn ein zweites Gerät die Konfiguration verwaltet, werden „Remote“ (Dezentral) sowie die Sicherheitsnetzwerknummer (SNN) und Netzknotenadresse oder Steckplatznummer der die Konfiguration verwaltenden Steuerung angezeigt. „Communication error“ (Kommunikationsfehler) wird angezeigt, wenn das Auslesen des Geräts misslingt.

Wenn Sie online geschaltet sind, können Sie das Gerät durch Klicken auf die Schaltfläche „Reset Ownership“ (Verwaltungsberechtigung zurücksetzen) auf seine werkseitige Konfiguration zurücksetzen.



HINWEIS Sie können die Verwaltungsberechtigung nicht zurücksetzen, wenn noch Änderungen an den Moduleigenschaften ausstehen oder eine Sicherheits-Task-Signatur bzw. eine Sicherheitssperre vorliegt.

Adressieren von Sicherheits-E/A-Daten

Wenn Sie ein Gerät zum E/A-Konfigurationsordner hinzufügen, erstellt die Anwendung Logix Designer automatisch Steuerungsbereichs-Tags für das Gerät.

E/A-Informationen werden als Tag-Satz angezeigt. Jedes Tag verwendet eine Datenstruktur, die vom Typ und von den Leistungsmerkmalen des E/A-Geräts abhängt. Der Name eines Tags basiert auf dem Namen des Geräts im System.

Adressformat eines Sicherheits-E/A-Moduls

Beispiel für das Adressformat eines Sicherheits-E/A-Moduls.

BEISPIEL Modulename:Type.Member

Tabelle 19 – Adressformat eines Sicherheits-E/A-Geräts

Bezeichnung	Bedeutung	
Modulename	Der Name des Sicherheits-E/A-Geräts	
Type	Datentyp	Eingang: I Ausgang: O
Member	Spezifische Daten des E/A-Geräts	
	Nur-Eingangsmodul	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members
	Nur-Ausgangsmodul	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:O.Output Members
	Kombinations-E/A	Modulename:I.RunMode Modulename:I.ConnectionFaulted Modulename:I.Input Members Modulename:O.Output Members

Adressformat von Kinetix 5500-, Kinetix 5700- und PowerFlex 527-Antrieben

Beispiel für das Adressformat von Kinetix 5500-, Kinetix 5700- und PowerFlex 527-Antrieben.

BEISPIEL Drivename:Type.Member

Tabelle 20 – Adressformat eines Antriebsicherheits-E/A-Geräts

Bezeichnung	Bedeutung	
Drivename	Der Name des Kinetix- oder PowerFlex-Antriebs	
Type	Datentyp	Eingang: SI Ausgang: SO
Member	Spezifische Daten des E/A-Geräts	
	Nur-Eingangsmodul	Drivename:SI.ConnectionStatus Drivename:SI.RunMode Drivename:SI.ConnectionFaulted Drivename:SI.Status Drivename:SI.TorqueDisabled Drivename:SI.SafetyFault Drivename:SI.ResetRequired
	Nur-Ausgangsmodul	Drivename:SO.Command Drivename:SO.SafeTorqueOff Drivename:SO.Reset

Tabelle 21 – Weitere Informationen

Quelle	Beschreibung
Kapitel 9, Zustandsüberwachung und Fehlerbehebung	Enthält Informationen zur Überwachung der Sicherheits-Tag-Daten
Steuerungen Logix5000 – E/A- und Tag-Daten – Programmierhandbuch, Publikation 1756-PM004	Enthält Informationen zur Adressierung von Standard-E/A-Geräten

Überwachen des Sicherheits-E/A-Gerätestatus

Sie können den Status des Sicherheits-E/A-Geräts über die explizite Nachrichtenübertragung oder über die Statusanzeigen der E/A-Module überwachen. Informationen zur Fehlerbehebung eines E/A-Moduls finden Sie in den unter Weitere Informationen auf Seite 14 aufgeführten Guard I/O-Benutzerhandbüchern.

Tabelle 22 – Statusanzeige für Guard E/A-Module

Anzeige	Status	Beschreibung		
		Guard I/O DeviceNet-Module	**Guard I/O EtherNet/IP-Module**	**POINT Guard I/O-Module**
Modulstatus (MS)	Aus	Keine Stromversorgung.		
	Grün, ein	Betrieb unter normalen Bedingungen.		
	Grün, blinkend	Gerät im Leerlauf.		
	Rot, blinkend	Ein korrigierbarer Fehler liegt vor.	Es liegt ein korrigierbarer Fehler vor oder es läuft ein Firmware-Update.	
	Rot, ein	Ein nicht korrigierbarer Fehler liegt vor.		
	Rot/Grün, blinkend	Selbsttest wird durchgeführt.	Es laufen Selbsttests oder das Modul ist nicht richtig konfiguriert. Weitere Informationen erhalten Sie über die Statusanzeige des Netzwerks.	
Netzwerkstatus (NS)	Aus	Gerät ist nicht online oder wird evtl. nicht mit Strom versorgt.		
	Grün, ein	Gerät ist online; Verbindungen sind aufgebaut.		
	Grün, blinkend	Gerät ist online; keine Verbindungen aufgebaut.		
	Rot, blinkend	Kommunikations-Timeout.	Kommunikations-Timeout oder es läuft ein Firmware-Update.	
	Rot, ein	Kommunikationsverlust. Das Gerät hat einen Fehler erkannt, der die Netzwerkkommunikation verhindert.		
	Rot/Grün, blinkend	Ein Kommunikationsfehler liegt vor oder die Sicherheitsnetzwerknummer (SNN) wird gerade festgelegt.	Selbsttest wird durchgeführt.	Nicht zutreffend.
Eingangspunkte (IN*x*)	Aus	Sicherheitseingang ist AUS.		
	Gelb, ein	Sicherheitseingang ist EIN.		
	Rot, ein	Ein Fehler ist in der Eingangsschaltung aufgetreten.		
	Rot, blinkend	Bei ausgewähltem Doppelkanalbetrieb ist ein Fehler in der Partnereingangsschaltung aufgetreten.		
Ausgangspunkte (O*x*)	Aus	Sicherheitsausgang ist AUS.		
	Gelb, ein	Sicherheitsausgang ist EIN.		
	Rot, ein	Ein Fehler ist in der Ausgangsschaltung aufgetreten.		
	Rot, blinkend	Bei ausgewähltem Doppelkanalbetrieb ist ein Fehler in der Partnerausgangsschaltung aufgetreten.		
Testausgangspunkte (T*x*)	Aus	Nicht zutreffend.	Der Ausgang ist AUS.	Nicht zutreffend.
	Gelb, ein		Der Ausgang ist EIN.	
	Rot, ein		Ein Fehler ist in der Ausgangsschaltung aufgetreten.	
LOCK	Gelb, ein	Gerätekonfiguration ist gesperrt.	Diese Funktion wird von der Anwendung Logix Designer nicht unterstützt.	
	Gelb, blinkend	Gerätekonfiguration ist gültig, aber Gerät ist nicht gesperrt.		
	Gelb, aus	Ungültig, keine Konfigurationsdaten oder das Gerät wurde konfiguriert.		
IN PWR	Grün, aus	Keine Leistungsaufnahme.		Nicht zutreffend.
	Grün, ein	Eingangsleistungsaufnahme erfüllt die Spezifikationen.		
	Gelb, ein	Eingangsleistungsaufnahme liegt außerhalb der Spezifikationen.		
OUT PWR	Grün, aus	Keine Ausgangsleistung.		
	Grün, ein	Ausgangsleistungsaufnahme erfüllt die Spezifikationen.		
	Gelb, ein	Ausgangsleistungsaufnahme liegt außerhalb der Spezifikationen.		
PWR	Grün, aus	Nicht zutreffend.		Keine Stromversorgung.
	Grün, ein			Leistungsaufnahme erfüllt die Spezifikationen.
	Gelb, ein			Leistungsaufnahme liegt außerhalb der Spezifikationen.

Weitere Informationen über die Statusanzeigen der Kinetix 5500-, Kinetix 5700- und PowerFlex 527-Antriebe siehe Seite 14.

Zurücksetzen eines Moduls auf die Werkseinstellungen

Wenn zuvor ein Guard I/O-Modul verwendet wurde, löschen Sie die vorherige Konfiguration durch Zurücksetzen des Moduls auf seine Werkseinstellung, bevor Sie es in ein Sicherheitsnetzwerk installieren.

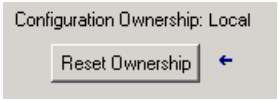
Wenn das Steuerungsprojekt online geschaltet ist, zeigt die Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Module Properties“ (Moduleigenschaften) die aktuellen Verwaltungsrechte an der Konfiguration an. Wenn das geöffnete Projekt die Verwaltungsberechtigung für die Konfiguration hat, wird „Local“ (Zentral) angezeigt. Wenn ein zweites Gerät die Konfiguration verwaltet, werden „Remote“ (Dezentral) sowie die Sicherheitsnetzwerknummer (SNN) und Netzknotenadresse oder Steckplatznummer des die Konfiguration verwaltenden Geräts angezeigt. „Communication error“ (Kommunikationsfehler) wird angezeigt, wenn das Auslesen des Moduls misslingt.

Wenn die Verbindung „Local“ (Zentral) ist, müssen Sie die Modulverbindung vor dem Zurücksetzen der Verwaltungsrechte sperren. Gehen Sie wie folgt vor, um das Modul zu sperren.

1. Klicken Sie mit der rechten Maustaste auf das Modul und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf die Registerkarte „Connection“ (Verbindung).
3. Wählen Sie „Inhibit Connection“ (Verbindung sperren) aus.
4. Klicken Sie auf „Apply“ (Anwenden) und anschließend auf „OK“.

Gehen Sie wie folgt vor, um das Modul im Online-Modus auf seine werkseitige Konfiguration zurückzusetzen.

1. Klicken Sie mit der rechten Maustaste auf das Modul und wählen Sie „Properties“ (Eigenschaften) aus.
2. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).
3. Klicken Sie auf „Reset Ownership“ (Verwaltungsberechtigung zurücksetzen).



Austauschen eines Geräts über die Anwendung Logix Designer

Sie können die Anwendung Logix Designer verwenden, um ein Sicherheits-E/A-Gerät in einem Ethernet-Netzwerk auszutauschen. Beim Austausch eines Guard I/O-Moduls in einem DeviceNet-Netzwerk hängt Ihre Auswahl vom Modultyp ab.

Tabelle 23 – Software

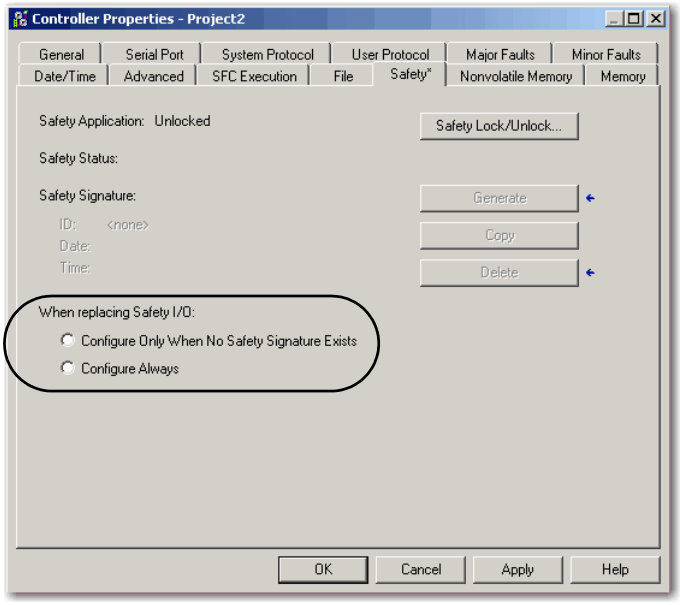
Verwendetes Modul	Zu verwendende Software	Siehe
Guard I/O-Modul der Serie 1791DS mit Adapter 1756-DNB	Anwendung Logix Designer	unten
POINT Guard I/O-Modul der Serie 1734 mit Adapter 1734-PDN	Software RSNetWorx for DeviceNet	Austauschen eines POINT Guard I/O-Moduls über die Software RSNetWorx for DeviceNet auf Seite 87

Wenn Sie auf einen Teil des CIP Safety-Systems angewiesen sind, um das SIL 3-Verhalten während des Austauschs und der Funktionsprüfung eines Geräts aufrechtzuerhalten, kann das Merkmal „Configure Always“ (Immer konfigurieren) nicht verwendet werden. Siehe Austausch bei aktivierter Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits- (Task-) Signatur vorliegt) auf Seite 82.

Falls Sie nicht auf das gesamte routingfähige CIP Safety-Steuerungssystem angewiesen sind, um das SIL 3/PLe-Verhalten während des Austauschs und der Funktionsprüfung eines Geräts aufrechtzuerhalten, kann das Merkmal „Configure Always“ (Immer konfigurieren) verwendet werden. Siehe Austausch bei aktivierter Option „Configure Always“ (Immer konfigurieren) auf Seite 86.

Der Austausch des Sicherheits-E/A-Geräts wird auf der Registerkarte „Safety“ (Sicherheit) der GuardLogix-Steuerung konfiguriert.

Abbildung 23 – Austauschen eines Sicherheits-E/A-Geräts



Austausch bei aktivierter Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits- (Task-) Signatur vorliegt)

Beim Austausch eines Sicherheits-E/A-Geräts wird die Konfiguration von der Sicherheitssteuerung heruntergeladen, wenn die Gerätekennung (DeviceID) des neuen Geräts mit der des ursprünglichen Geräts übereinstimmt. Die Gerätekennung setzt sich aus der Knoten-/IP-Adresse und der Sicherheitsnetzwerknummer (SNN) zusammen. Sie wird immer aktualisiert, wenn die SNN konfiguriert wird.

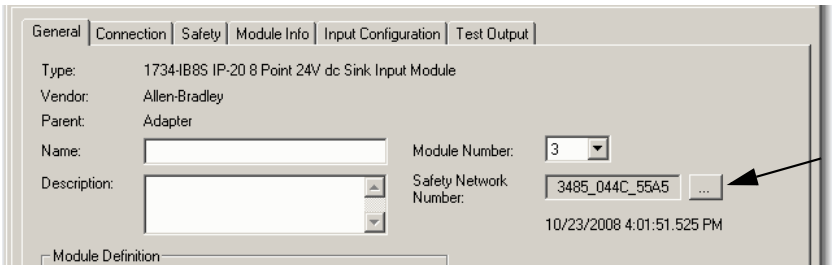
Wenn für das Projekt die Option „Configure Only When No Safety (Task) Signature Exists“ (Nur konfigurieren, wenn keine Sicherheits-(Task-) Signatur vorliegt) ausgewählt ist, wenden Sie die in Tabelle 24 beschriebene geeignete Vorgehensweise an, um das Sicherheits-E/A-Gerät auf Grundlage Ihres Szenarios auszutauschen. Wenn Sie die beschriebenen Schritte ordnungsgemäß durchgeführt haben, stimmt die Gerätekennung mit der ursprünglichen ID überein, wodurch die Sicherheitssteuerung in der Lage ist, die richtige Gerätekonfiguration herunterzuladen. Anschließend wird die Sicherheitsverbindung erneut hergestellt.

Tabelle 24 – Austauschen eines Moduls

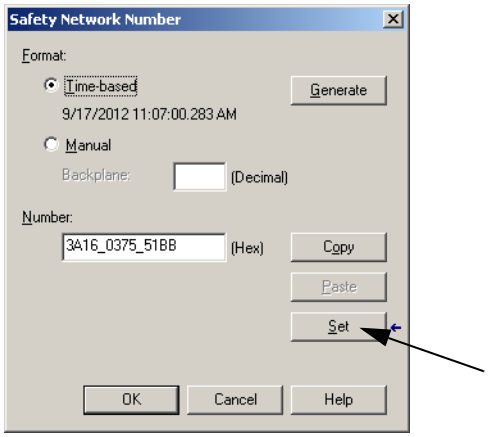
GuardLogix-Sicherheitssignatur vorhanden	Zustand Austauschmodule	Erforderliche Maßnahme
Nein	Keine SNN (Werkseinstellungen)	Keine. Das Gerät ist einsatzbereit.
Ja oder Nein	Gleiche SNN wie ursprüngliche Sicherheits-Task-Konfiguration	Keine. Das Gerät ist einsatzbereit.
Ja	Keine SNN (Werkseinstellungen)	Siehe Szenario 1 – Austauschgerät ist im Werkszustand und Sicherheitssignatur liegt vor auf Seite 83.
Ja	Andere SNN als ursprüngliche Sicherheits-Task-Konfiguration	Siehe Szenario 2 – Austauschgerät hat andere SNN als ursprüngliches Gerät und Sicherheitssignatur liegt vor auf Seite 84.
Nein		Siehe Szenario 3 – Austauschgerät hat andere SNN als ursprüngliches Gerät und Sicherheitssignatur liegt nicht vor auf Seite 86.

Szenario 1 – Austauschgerät ist im Werkszustand und Sicherheitssignatur liegt vor

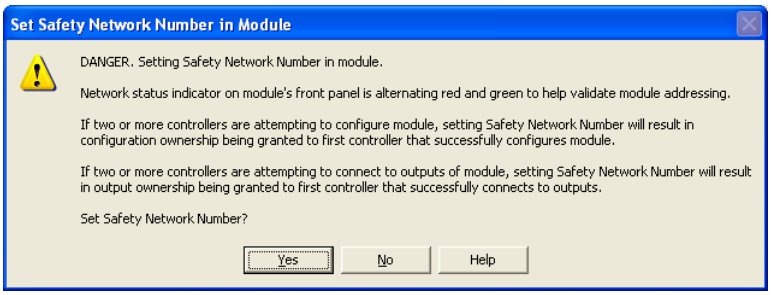
1. Entfernen Sie das alte E/A-Gerät, und installieren Sie das neue Gerät.
2. Klicken Sie mit der rechten Maustaste auf das neue Sicherheits-E/A-Gerät und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.



4. Klicken Sie auf „Set“ (Festlegen).



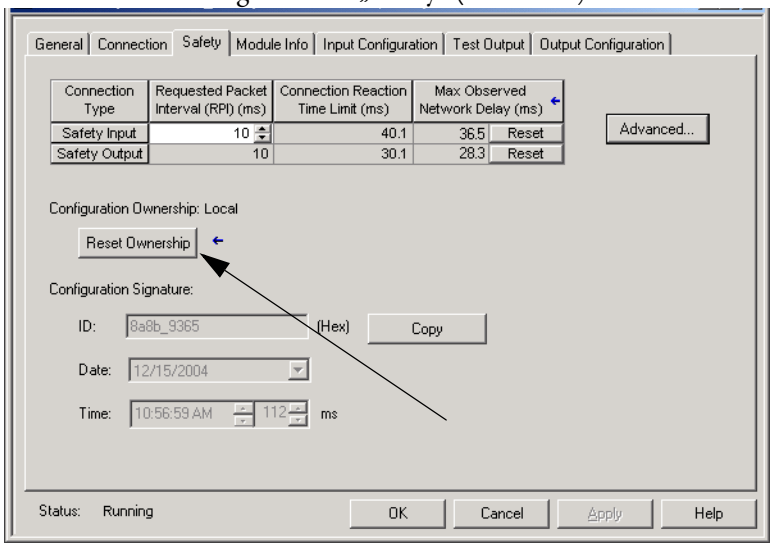
5. Vergewissern Sie sich, dass die Statusanzeige für den Netzwerkstatus (NS) am richtigen Gerät abwechselnd rot und grün aufleuchtet, bevor Sie im Bestätigungsdialogfeld auf „Yes“ (Ja) klicken, um die SNN festzulegen und das Austauschgerät zu übernehmen.



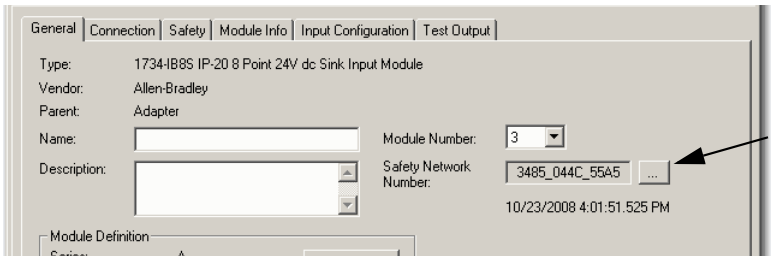
6. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Gerät und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Szenario 2 – Austauschgerät hat andere SNN als ursprüngliches Gerät und Sicherheitssignatur liegt vor

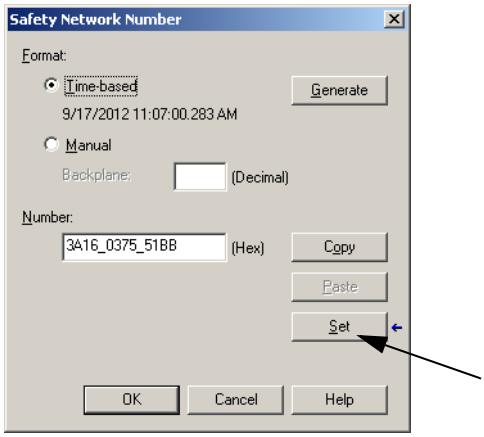
1. Entfernen Sie das alte E/A-Gerät und installieren Sie das neue Gerät.
2. Klicken Sie mit der rechten Maustaste auf das Sicherheits-E/A-Gerät und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



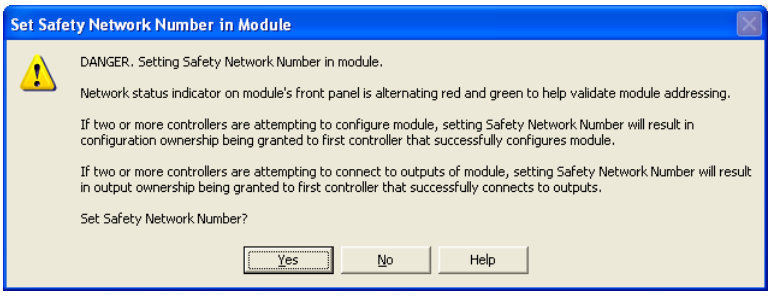
4. Klicken Sie auf „Reset Ownership“ (Verwaltungsberechtigung zurücksetzen).
5. Klicken Sie auf „OK“.
6. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie „Properties“ (Eigenschaften) aus.
7. Klicken Sie rechts neben der Sicherheitsnetzwerknummer auf die Schaltfläche ..., um das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) aufzurufen.



8. Klicken Sie auf „Set“ (Festlegen).



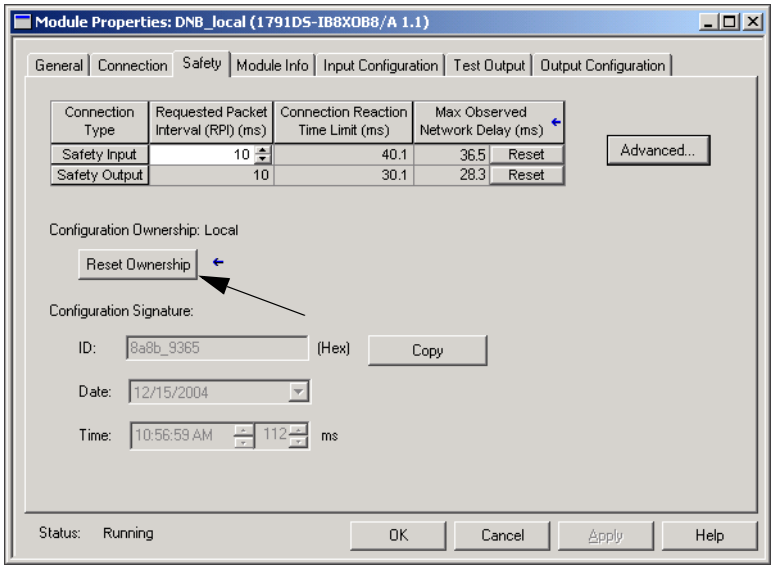
9. Vergewissern Sie sich, dass die Statusanzeige für den Netzwerkstatus (NS) am richtigen Gerät abwechselnd rot und grün aufleuchtet, bevor Sie im Bestätigungsdialogfeld auf „Yes“ (Ja) klicken, um die SNN festzulegen und das Austauschgerät zu übernehmen.



10. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Gerät und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Szenario 3 – Austauschgerät hat andere SNN als ursprüngliches Gerät und Sicherheitssignatur liegt nicht vor

1. Entfernen Sie das alte E/A-Gerät und installieren Sie das neue Gerät.
2. Klicken Sie mit der rechten Maustaste auf das Sicherheits-E/A-Gerät und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



4. Klicken Sie auf „Reset Ownership“ (Verwaltungsberechtigung zurücksetzen).
5. Klicken Sie auf „OK“.
6. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Gerät und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Austausch bei aktivierter Option „Configure Always“ (Immer konfigurieren)

ACHTUNG: Aktivieren Sie die Option „Configure Always“ (Immer konfigurieren) nur, wenn die Beibehaltung des SIL 3-Verhaltens während des Austauschs und der Funktionstests eines Geräts **nicht** vom gesamten CIP Safety-Steuerungssystem abhängt.

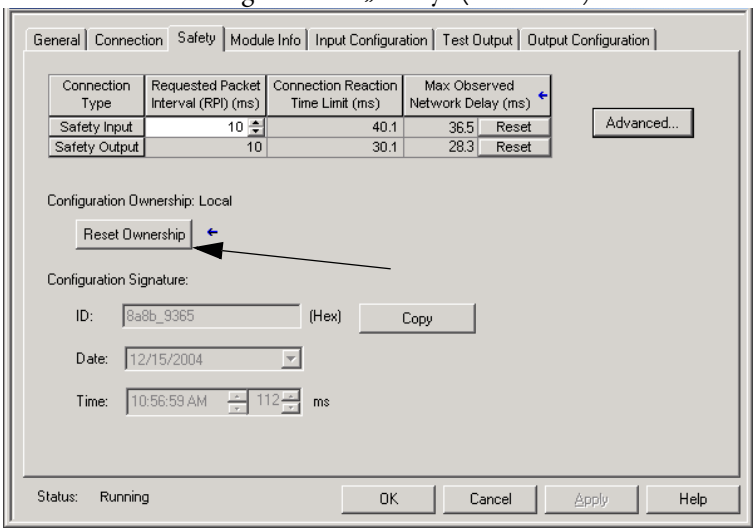
Installieren Sie Geräte im Werkszustand in einem CIP Safety-Netzwerk bei aktivierter Funktion „Configure Always“ (Immer konfigurieren) nur, wenn Sie dieses Austauschverfahren befolgen.

Wenn die Option „Configure Always“ (Immer konfigurieren) im Steuerungsprojekt aktiviert ist, sucht die Steuerung automatisch ein Austauschgerät, das den folgenden Anforderungen entspricht, und stellt eine Verbindung zu diesem her:

- Die Steuerung hat an dieser Netzwerkadresse Konfigurationsdaten für ein kompatibles Gerät.
- Das Gerät befindet sich im Werkszustand oder verfügt über eine SNN, die mit der Konfiguration übereinstimmt.

Wenn für die Projektkonfiguration die Option „Configure Always“ (Immer konfigurieren) aktiviert ist, wenden Sie die entsprechende Vorgehensweise zum Austausch eines Sicherheits-E/A-Geräts an.

1. Entfernen Sie das alte E/A-Gerät und installieren Sie das neue Gerät.
   a. Befindet sich das Gerät im Werkszustand, fahren Sie mit Schritt 6 fort.
   Es muss keine Maßnahme ergriffen werden, damit die GuardLogix-Steuerung die Verwaltungsberechtigung für das Gerät erhält.
   b. Tritt ein Fehler aufgrund nicht übereinstimmender SNN auf, fahren Sie mit dem nächsten Schritt fort, um das Gerät in den Werkszustand zurückzusetzen.
2. Klicken Sie mit der rechten Maustaste auf das Sicherheits-E/A-Gerät und wählen Sie „Properties“ (Eigenschaften) aus.
3. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).



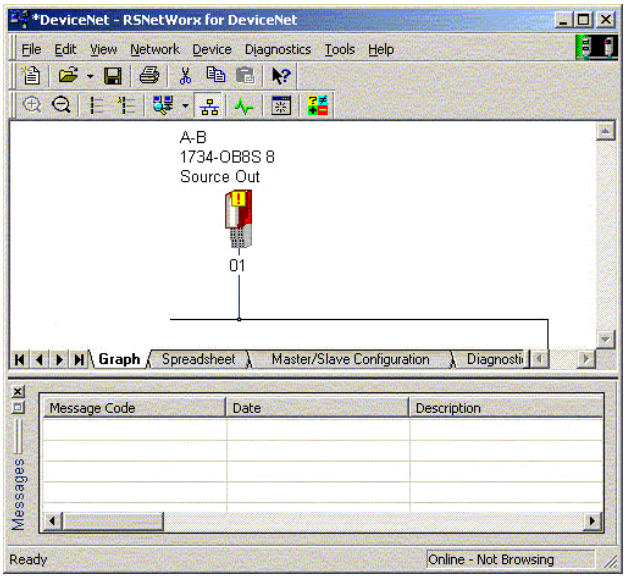
4. Klicken Sie auf „Reset Ownership“ (Verwaltungsberechtigung zurücksetzen).
5. Klicken Sie auf „OK“.
6. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Gerät und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Austauschen eines POINT Guard I/O-Moduls über die Software RSNetWorx for DeviceNet

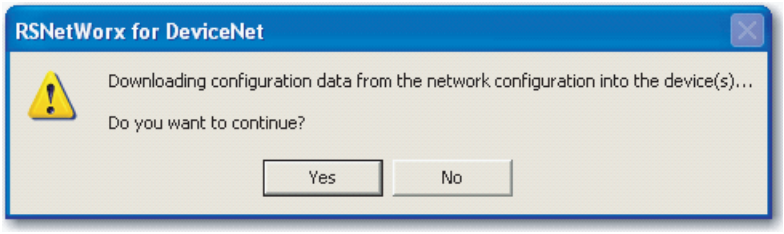
Gehen Sie wie im Folgenden beschrieben vor, um ein POINT Guard I/O-Modul auszutauschen, wenn das Modul und die Steuerung auf einem DeviceNet-Netzwerk betrieben werden.

1. Tauschen Sie das Modul aus und stimmen Sie die Knotennummer mit der des ursprünglichen Moduls ab.
2. Öffnen Sie Ihr Projekt in der Software RSNetWorx for DeviceNet.

   Befindet sich das Austauschmodul im Werkszustand oder verfügt es über eine SNN, die nicht mit der des ursprünglichen Moduls übereinstimmt, ist das Modul mit einem Ausrufzeichen versehen.

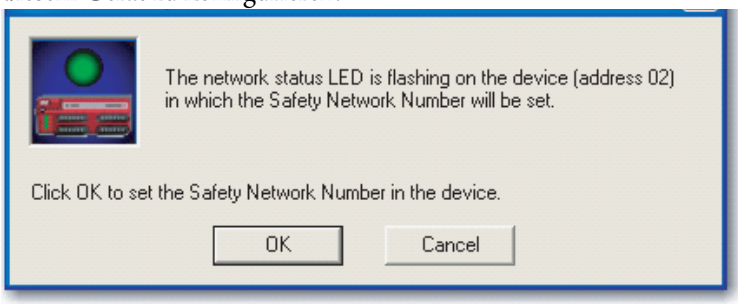


3. Klicken Sie mit der rechten Maustaste auf das Modul und wählen „Download to Device“ (Auf Gerät herunterladen).



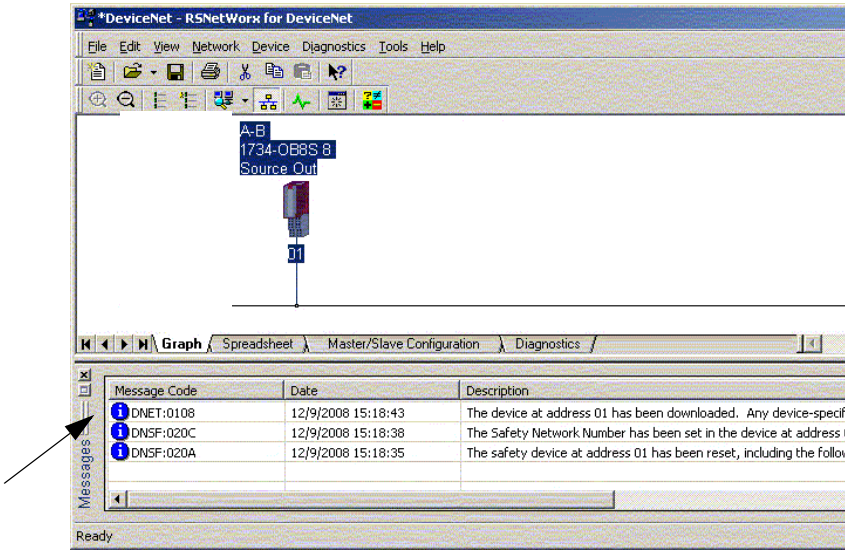
4. Klicken Sie auf „Yes“ (Ja), um den Vorgang zu bestätigen.
5. Klicken Sie auf „Download“ (Herunterladen) im Dialogfeld „Safety Network Number Mismatch“ (Nicht übereinstimmende Sicherheitsnetzwerknummer), um die SNN auf dem Austauschmodul zu konfigurieren.

6. Vergewissern Sie sich, dass die Anzeige für den Netzwerkstatus (NS) am richtigen Modul blinkt, und klicken Sie auf „OK“, um die SNN auf diesem Gerät zu konfigurieren.



Die Software RSNetWorx for DeviceNet bestätigt, dass die SNN konfiguriert wurde.

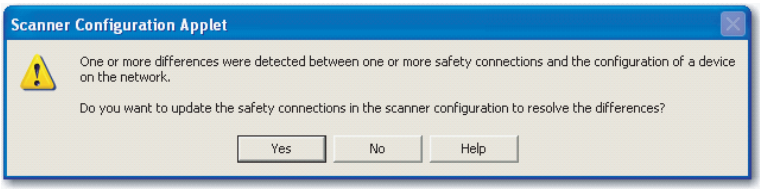
Nach dem erfolgreichen Herunterladen zeigt das Hauptprojekt die folgende Meldung an: „The device at address *xx* has been downloaded. Any device-specific messages related to the download operation are displayed separately.“ (Das Gerät an Adresse xx wurde heruntergeladen. Alle gerätespezifischen Meldungen im Zusammenhang mit dem Download-Vorgang werden separat angezeigt.)



Angenommen, dass dies die richtige Konfiguration von der ursprünglichen DNT-Datei ist, stimmen die SNN und die Konfigurationssignatur nun mit der ursprünglichen SNN bzw. Signatur überein. Wenn bereits ein Anschluss an die Steuerung besteht, wird eine Verbindung hergestellt. Die Steuerung kann im Run-Modus verbleiben, während die Konfiguration auf das Austauschmodul heruntergeladen wird.

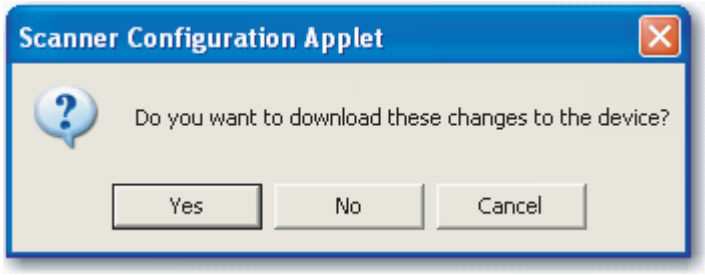
Wenn Sie diese Konfiguration auf eine temporäre Einrichtung herunterladen, stellen Sie das Modul ins Netzwerk, wo es automatisch eine Verbindung zur Steuerung herstellt.

Stammt die auf das Modul heruntergeladene Konfiguration nicht von der ursprünglichen DNT-Datei, stimmt die Konfigurationssignatur nicht mit der ursprünglichen Signatur überein. Auch wenn Sie dieselben Parameter in einer neuen DNT-Datei erzeugen, unterscheiden sich die Zeit- und Datumsanteile der Signatur, so dass die Verbindung zur Steuerung nicht hergestellt wird. Klicken Sie in diesem Fall auf die Registerkarte „Safety Connection“ (Sicherheitsverbindung) für die Steuerung, die meldete, dass eine andere Konfigurationssignatur vorliegt. Ihnen wird dann die Option angeboten, die neue Konfigurationssignatur abzustimmen. Sie sollten jedoch zuerst das Sicherheitssystem erneut validieren, da nicht die ursprüngliche DNT-Datei verwendet wird.



7. Klicken Sie auf „Yes“ (Ja).

   Dadurch wird der Run-Modus der Steuerung beendet und Sie werden aufgefordert, die Änderungen herunterzuladen.



8. Klicken Sie auf „Yes“ (Ja), um die neue Verbindungskonfiguration auf die Steuerung herunterzuladen.

   Nach dem Download wechselt die Steuerung wieder zurück in den Run-Modus und die Verbindung zum Austauschmodul wird hergestellt.

9. Befolgen Sie die vom Hersteller vorgeschriebene Vorgehensweise, nach der das ausgetauschte E/A-Modul und das System einer Funktionsprüfung unterzogen werden und das System für den Betrieb freigegeben wird.

Entwicklung von Sicherheitsanwendungen

Thema	Seite
Die Sicherheits-Task	92
Sicherheitsprogramme	93
Sicherheitsroutinen	94
Sicherheits-Tags	94
Produzierte/konsumierte Sicherheits-Tags	98
Zuordnen von Sicherheits-Tags	104
Schutz von Sicherheitsanwendungen	106
Einschränkungen bei der Programmierung	110

In diesem Kapitel werden die Komponenten erläutert, aus denen ein Sicherheitsprojekt besteht. Es bietet Informationen zur Verwendung der Funktionen, die die Integrität der Sicherheitsanwendung schützen, wie z. B. die Sicherheits-Task-Signatur und die Sicherheitssperre.

Informationen zu Richtlinien und Anforderungen für die Entwicklung und Inbetriebnahme von SIL 3- und PLe-Sicherheitsanwendungen enthält die Publikation 1756-RM099, Steuerungssysteme GuardLogix 5570 – Sicherheitsreferenzhandbuch.

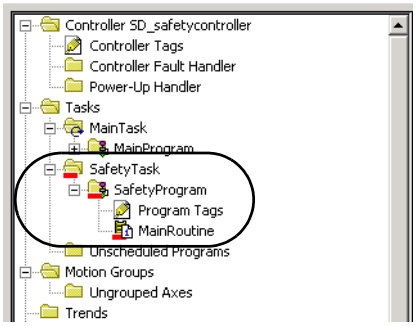
Das Sicherheitsreferenzhandbuch beinhaltet folgende Themen:

- Erstellen einer detaillierten Projektspezifikation
- Schreiben, Dokumentieren und Testen der Anwendung
- Generieren der Sicherheits-Task-Signatur, um das Projekt zu identifizieren und zu schützen
- Bestätigen des Projekts durch Ausdruck oder Anzeige des hochgeladenen Projekts und durch manuelles Vergleichen der Konfigurationen, Sicherheitsdaten und der Sicherheitsprogrammlogik
- Verifizieren des Projekts durch Prüffälle, Simulationen, Funktionsverifikationsprüfungen und eine unabhängige Sicherheitsüberprüfung, falls erforderlich
- Sperren der Sicherheitsanwendung
- Berechnen der Reaktionszeit des Systems

Die Sicherheits-Task

Wenn Sie ein Sicherheitssteuerungsprojekt erstellen, generiert die Anwendung Logix Designer automatisch eine einzige Sicherheits-Task mit einem Sicherheitsprogramm und einer (sicherheitsbezogenen) Hauptroutine.

Abbildung 24 – Sicherheits-Task im Controller Organizer (Steuerungsorganisator)



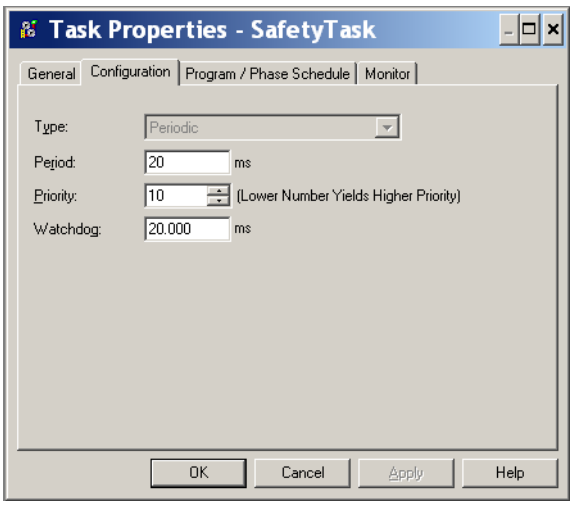
Innerhalb der Sicherheits-Task können Sie mehrere Sicherheitsprogramme verwenden, die aus mehreren Sicherheitsroutinen bestehen. Die GuardLogix-Steuerung unterstützt eine Sicherheits-Task. Die Sicherheits-Task kann nicht gelöscht werden.

Innerhalb der Sicherheits-Task können Sie keine Standardprogramme planen oder Standardroutinen ausführen.

Spezifizieren der Sicherheits-Task-Zeitspanne

Die Sicherheits-Task ist eine periodische/zeitgesteuerte Task. Sie legen die Task-Priorität und den Überwachungszeitraum über das Dialogfeld „Task Properties – Safety Task“ (Task-Eigenschaften – Sicherheits-Task) fest. Öffnen Sie das Dialogfeld, indem Sie mit der rechten Maustaste auf die Sicherheits-Task klicken und dann „Properties“ (Eigenschaften) auswählen.

Abbildung 25 – Konfigurieren der Zeitspanne für die Sicherheits-Task



Die Sicherheits-Task hat die Priorität „Hoch“. Sie geben sowohl die Zeitspanne der Sicherheits-Task (in ms) als auch den Überwachungszeitraum (Watchdog) der Sicherheits-Task (in ms) an. Die Sicherheits-Task-Zeitspanne ist der Zeitraum, in dem die Sicherheits-Task ausgeführt wird. Der Überwachungszeitraum der Sicherheits-Task ist die maximale, zugelassene Zeit vom Start der Ausführung der Sicherheits-Task bis zu deren Beendigung.

Die Zeitspanne der Sicherheits-Task ist begrenzt auf ein Maximum von 500 ms und kann online nicht geändert werden. Stellen Sie sicher, dass der Sicherheits-Task genügend Zeit zum Abschluss der Logikausführung bleibt, bevor sie erneut ausgelöst wird. Wenn während des Überwachungszeitraums für die Sicherheits-Task ein Timeout auftritt, wird ein nicht korrigierbarer Sicherheitsfehler in der Sicherheitssteuerung generiert.

Die Zeitspanne für die Sicherheits-Task wirkt sich direkt auf die Reaktionszeit des Systems aus.

Die Publikation 1756-RM099, Steuerungssysteme GuardLogix 5570 – Sicherheitsreferenzhandbuch, enthält detaillierte Informationen zur Berechnung der Reaktionszeit des Systems.

Ausführen der Sicherheits-Task

Die Sicherheits-Task wird genau so ausgeführt wie eine periodische Standard-Task, allerdings mit folgenden Ausnahmen:

- Die Sicherheits-Task beginnt mit der Ausführung erst, wenn die Primärsteuerung und der Sicherheitspartner ihre Steuerungspartnerschaft festlegen. (Standard-Tasks beginnen mit der Ausführung, sobald die Steuerung in den Run-Modus wechselt.)
- Alle Sicherheitseingangs-Tags (Eingänge, konsumiert und zugeordnet) werden aktualisiert und zu Beginn der Ausführung der Sicherheits-Task eingefroren.

  Auf Seite 104 finden Sie weitere Informationen über die Zuordnung von Sicherheits-Tags.

- Die Werte der Sicherheitsausgangs-Tags (ausgegeben und produziert) werden nach Abschluss der Ausführung der Sicherheits-Task aktualisiert.

Sicherheitsprogramme

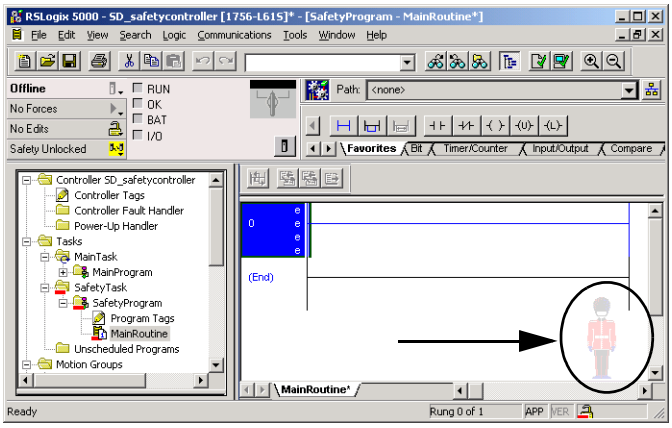
Sicherheitsprogramme besitzen sämtliche Attribute eines Standardprogramms, werden jedoch in der Sicherheits-Task geplant und können nur Sicherheitskomponenten enthalten. Sicherheitsprogramme können nur Sicherheitsroutinen enthalten. Eine Sicherheitsroutine muss als Hauptroutine und eine andere kann als Fehlerroutine festgelegt sein.

Sicherheitsprogramme können keine Standardroutinen oder Standard-Tags enthalten.

Sicherheitsroutinen

Sicherheitsroutinen besitzen sämtliche Attribute einer Standardroutine, sind jedoch nur in einem Sicherheitsprogramm vorhanden. Momentan wird für Sicherheitsroutinen nur die Kontaktplanlogik unterstützt.

HINWEIS Ein Wasserzeichen ermöglicht die visuelle Unterscheidung zwischen einer Sicherheitsroutine und einer Standardroutine.



Sicherheits-Tags

Ein Tag ist ein Bereich im Speicher der Steuerung, in dem Daten gespeichert werden. Tags sind der grundlegende Mechanismus zur Speicherzuweisung, zur Bezugnahme auf Daten aus der Logik sowie zur Datenüberwachung. Sicherheits-Tags besitzen alle Attribute von Standard-Tags sowie zusätzliche zertifizierte Mechanismen zur Sicherstellung der SIL 3-Datenintegrität.

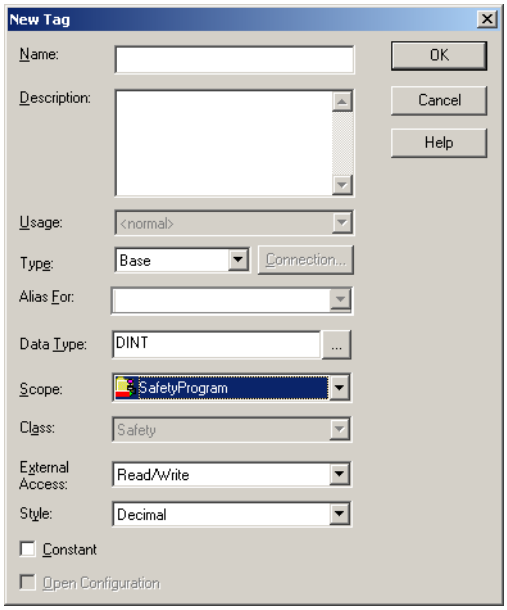
Folgende Eigenschaften sind einem Tag bei seiner Erstellung zuzuweisen:

- Name
- Beschreibung (optional)
- Tag-Typ
- Datentyp
- Bereich
- Klasse
- Stil
- Externer Zugriff

Sie können auch angeben, ob der Tag-Wert eine Konstante sein soll.

Öffnen Sie zum Erstellen eines Sicherheits-Tags das Dialogfeld „New Tag“ (Neues Tag), indem Sie mit der rechten Maustaste auf „Controller Tags“ (Steuerungs-Tags) oder „Program Tags“ (Programm-Tags) klicken und „New Tag“ (Neues Tag) auswählen.

Abbildung 26 – Erstellen eines neuen Tags



Tag-Typ

In Tabelle 25 werden die vier Tag-Typen definiert:

Tabelle 25 – Vier Tag-Typen

Tag-Typ	Beschreibung
Basis-Tag	Diese Tags speichern Werte, die von der Logik innerhalb des Projekts verwendet werden.
Alias-Tag	Ein Tag, das auf ein anderes Tag hinweist. Ein Alias-Tag kann auf ein anderes Alias-Tag oder ein Basis-Tag hinweisen. Ein Alias-Tag kann sich auch auf eine Komponente eines anderen Tags beziehen, indem es auf ein Glied einer Struktur verweist, ein Datenfeldelement oder ein Bit innerhalb eines Tags oder eines Glieds. **WICHTIG:** Verwenden Sie Alias-Tags nicht zwischen Standard- und Sicherheits-Tags in Sicherheitsanwendungen. Stattdessen ermöglicht die entsprechende Sicherheits-Tag-Zuordnungsfunktion eine Zuordnung von Standard-Tags zu Sicherheits-Tags. Siehe Zuordnen von Sicherheits-Tags auf Seite 104.
Produziertes Tag	Ein Tag, das von einer Steuerung für die Verwendung durch andere Steuerungen zur Verfügung gestellt wird. Maximal 15 Steuerungen können gleichzeitig Daten konsumieren (empfangen). Ein produziertes Tag sendet seine Daten an ein oder mehrere konsumierende Tag(s) ohne Verwendung von Logik. Die produzierten Tag-Daten werden mit dem RPI des konsumierenden Tags übermittelt.
Konsumiertes Tag	Ein Tag, das Daten eines produzierten Tags empfängt. Der Datentyp des konsumierten Tags muss mit dem Datentyp des produzierten Tags übereinstimmen. Das angeforderte Paketintervall (RPI) des konsumierten Tags bestimmt den Zeitraum, in dem die Daten aktualisiert werden.

Datentyp

Der Datentyp definiert den Datentyp, den das Tag speichert, wie z. B. Bit oder Ganzzahl.

Datentypen können zu Strukturen kombiniert werden. Eine Struktur stellt einen eindeutigen Datentyp zur Verfügung, der mit einer bestimmten Anforderung übereinstimmt. Innerhalb einer Struktur wird jeder individuelle Datentyp als Glied bezeichnet. Wie Tags haben auch Glieder einen Namen und einen Datentyp. Sie können Ihre eigenen Strukturen als benutzerdefinierte Datentypen erstellen.

Logix-Steuerungen enthalten vordefinierte Datentypen für die Verwendung mit spezifischen Befehlen.

Diese Datentypen sind für Sicherheits-Tags zulässig.

Tabelle 26 – Gültige Datentypen für Sicherheits-Tags

AUX_VALVE_CONTROL	DCI_STOP_TEST_MUTE	MANUAL_VALVE_CONTROL
BOOL	DINT	MUTING_FOUR_SENSOR_BIDIR
CAM_PROFILE	DIVERSE_INPUT	MUTING_TWO_SENSOR_ASYM
CAMSHAFT_MONITOR	EIGHT_POS_MODE_SELECTOR	MUTING_TWO_SENSOR_SYM
CB_CONTINUOUS_MODE	EMERGENCY_STOP	MOTION_INSTRUCTION
CB_CRANKSHAFT_POS_MONITOR	ENABLE_PENDANT	PHASE
CB_INCH_MODE	EXT_ROUTINE_CONTROL	PHASE_INSTRUCTION
CB_SINGLE_STROKE_MODE	EXT_ROUTINE_PARAMETERS	REDUNDANT_INPUT
CONFIGURABLE_ROUT	FBD_BIT_FIELD_DISTRIBUTE	REDUNDANT_OUTPUT
CONNECTION_STATUS	FBD_CONVERT	SAFETY_MAT
CONTROL	FBD_COUNTER	SERIAL_PORT_CONTROL
COUNTER	FBD_LOGICAL	SFC_ACTION
DCA_INPUT	FBD_MASK_EQUAL	SFC_STEP
DCAF_INPUT	FBD_MASKED_MOVE	SFC_STOP
DCI_MONITOR	FBD_TIMER	SINT
DCI_START	FIVE_POS_MODE_SELECTOR	STRING
DCI_STOP	INT	THRS_ENHANCED
DCI_STOP_TEST	LIGHT_CURTAIN	TIMER
DCI_STOP_TEST_LOCK	MAIN_VALVE_CONTROL	TWO_HAND_RUN_STATION

Bereich

Der Bereich eines Tags legt fest, wo Sie Zugriff auf die Tag-Daten haben. Wenn Sie ein Tag erstellen, definieren Sie dieses als Steuerungs-Tag (globale Daten) oder als Programm-Tag für ein spezifisches Sicherheitsprogramm oder ein Standardprogramm (lokale Daten). Sicherheits-Tags können Steuerungsbereichs- oder Sicherheitsprogrammbereichs-Tags sein.

Steuerungsbereichs-Tags

Bei den Steuerungsbereichs-Tags haben sämtliche Programme Zugriff auf die Sicherheitsdaten. Steuerungsbereichs-Tags sind notwendig, wenn sie:

- in mehr als einem Programm des Projekts verwendet werden.
- zum Produzieren oder Konsumieren von Daten verwendet werden.
- für die Kommunikation mit einem PanelView™-Terminal verwendet werden.
- zum Zuordnen von Sicherheits-Tags verwendet werden.

  Weitere Informationen finden Sie unter Zuordnen von Sicherheits-Tags auf Seite 104.

Steuerungsbereichs-Sicherheits-Tags können von Standardroutinen gelesen, aber nicht geschrieben werden.

WICHTIG	Steuerungsbereichs-Sicherheits-Tags können von jeder Standardroutine gelesen werden. Die Aktualisierungsgeschwindigkeit des Sicherheits-Tags basiert auf der Zeitspanne der Sicherheits-Task.

Die mit Sicherheits-E/A und produzierten oder konsumierten Sicherheitsdaten assoziierten Tags müssen Steuerungsbereichs-Sicherheits-Tags sein. Für produzierte/konsumierte Sicherheits-Tags müssen Sie einen benutzerdefinierten Datentyp erstellen, wobei das erste Glied der Tag-Struktur für den Status der Verbindung reserviert ist. Dieses Glied ist ein vordefinierter Datentyp mit dem Namen CONNECTION_STATUS.

Tabelle 27 – Weitere Informationen

Quelle	Beschreibung
Sicherheitsverbindungen auf Seite 127	Enthält weitere Informationen zum Glied CONNECTION_STATUS (VERBINDUNGS_STATUS)
Steuerungen Logix5000 – E/A- und Tag-Daten – Programmierhandbuch, Publikation 1756-PM004	Enthält Anweisungen zur Erstellung benutzerdefinierter Datentypen

Programmbereichs-Tags

Bei Programmbereichs-Tags werden die Daten von den anderen Programmen isoliert. Die Wiederverwendung von Programmbereichs-Tag-Namen zwischen Programmen ist erlaubt.

Programmbereichs-Sicherheits-Tags können nur über eine Sicherheitsroutine in demselben Sicherheitsprogramm gelesen oder geschrieben werden.

Klasse

Tags können als Standard- oder als Sicherheits-Tags klassifiziert werden. Tags, die als Sicherheits-Tags klassifiziert sind, müssen über einen Datentyp verfügen, der für Sicherheits-Tags zulässig ist.

Wenn Sie Programmbereichs-Tags erstellen, wird die Klasse automatisch spezifiziert, und zwar abhängig davon, ob das Tag in einem Standard- oder einem Sicherheitsprogramm erstellt wurde.

Wenn Sie Steuerungsbereichs-Tags erstellen, müssen Sie die Tag-Klasse manuell auswählen.

Konstanter Wert

Wenn Sie ein Tag als konstanten Wert festlegen, kann dieses nicht durch die Logik in der Steuerung oder durch eine externe Anwendung wie z. B. eine Bedienerschnittstelle geändert werden. Tags mit konstanten Werten können nicht geforct werden.

Über die Anwendung Logix Designer können konstante Standard-Tags und Sicherheits-Tags geändert werden, sofern keine Sicherheits-Task-Signatur vorliegt. Sicherheits-Tags können nicht geändert werden, wenn eine Sicherheits-Task-Signatur vorliegt.

Externer Zugriff

Der externe Zugriff definiert die Zugriffsebene, die für ein externes Gerät, wie z. B. eine Bedienerschnittstelle (HMI), zum Anzeigen oder Ändern von Tag-Werten zulässig ist. Der Zugriff über die Anwendung Logix Designer wird durch diese Einstellung nicht beeinflusst. Standardmäßig ist der Lese-/Schreibzugriff aktiviert.

Tabelle 28 – Stufen für externen Zugriff

Einstellung für externen Zugriff	Beschreibung
None (Ohne)	Von außerhalb der Steuerung kann nicht auf Tags zugegriffen werden.
Read Only (Schreibgeschützt)	Die Tags können durchsucht und angezeigt werden. Von außerhalb der Steuerung sind jedoch keine Änderungen an diesen Tags möglich.
Read/Write (Lese-/Schreibzugriff)	Die Standard-Tags können von außerhalb der Steuerung durchsucht, angezeigt und geändert werden.

Für Alias-Tags entspricht der Typ des externen Zugriffs dem Typ, der für das Basis-Ziel-Tag konfiguriert wurde.

Produzierte/konsumierte Sicherheits-Tags

Um Sicherheitsdaten zwischen GuardLogix-Steuerungen zu übertragen, müssen Sie produzierte und konsumierte Sicherheits-Tags verwenden. Alle produzierten und konsumierten Tags erfordern eine Verbindung. Der Standardverbindungstyp für produzierte und konsumierte Tags ist Unicast.

Tabelle 29 – Produzierte und konsumierte Verbindungen

Tag	Beschreibung der Verbindung
Produziert	Eine GuardLogix-Steuerung kann Sicherheits-Tags für andere GuardLogix-Steuerungen der Serie 1756 oder 1768 produzieren (an diese senden). Die produzierende Steuerung verwendet für jeden Consumer eine einzelne Verbindung.
Konsumiert	GuardLogix-Steuerungen können Sicherheits-Tags von anderen GuardLogix-Steuerungen der Serie 1756 oder 1768 konsumieren (empfangen). Jedes konsumierte Tag konsumiert eine Verbindung.

Produzierte und konsumierte Sicherheits-Tags unterliegen den folgenden Einschränkungen:

- Nur auf Steuerungsbereichs-Sicherheits-Tags kann gemeinsam zugegriffen werden.
- Produzierte und konsumierte Sicherheits-Tags sind auf 128 Byte begrenzt.

- Produzierte/konsumierte Tag-Paare müssen den gleichen benutzerdefinierten Datentyp haben.
- Das erste Glied dieses benutzerdefinierten Datentyps muss vom vordefinierten Datentyp CONNECTION_STATUS sein.
- Das angeforderte Paketintervall (RPI) des konsumierten Sicherheits-Tags muss der Zeitspanne der Sicherheits-Task der produzierenden GuardLogix-Steuerung entsprechen.

Die richtige Konfiguration produzierter und konsumierter Sicherheits-Tags für die gemeinsame Datennutzung zwischen Peer-Sicherheitssteuerungen erfordert das richtige Konfigurieren der Peer-Sicherheitssteuerungen, das Produzieren eines Sicherheits-Tags und das Konsumieren eines Sicherheits-Tags, wie nachfolgend beschrieben.

Konfigurieren der Sicherheitsnetzwerknummern von Peer-Sicherheitssteuerungen

Die Peer-Sicherheitssteuerung unterliegt den gleichen Konfigurationsanforderungen wie die lokale Sicherheitssteuerung. Die Peer-Sicherheitssteuerung muss ebenfalls über eine Sicherheitsnetzwerknummer (SNN) verfügen. Die SNN der Peer-Sicherheitssteuerung hängt von deren Position im System ab.

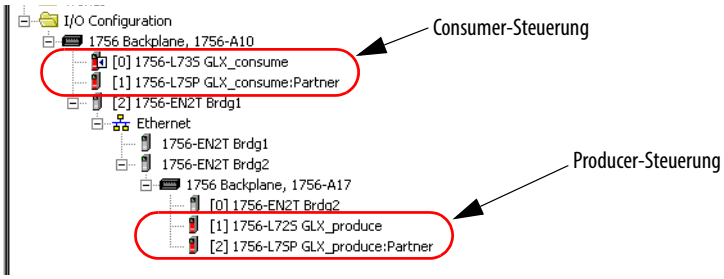
Tabelle 30 – SNN und Steuerungsposition

Position der Peer-Sicherheitssteuerung	SNN
Im lokalen Chassis	GuardLogix-Steuerungen, die sich im selben Chassis befinden, haben auch dieselbe SNN.
In einem anderen Chassis	Die Steuerung muss über eine eindeutige SNN verfügen.

Gehen Sie wie folgt vor, um die SNN zu kopieren und einzufügen.

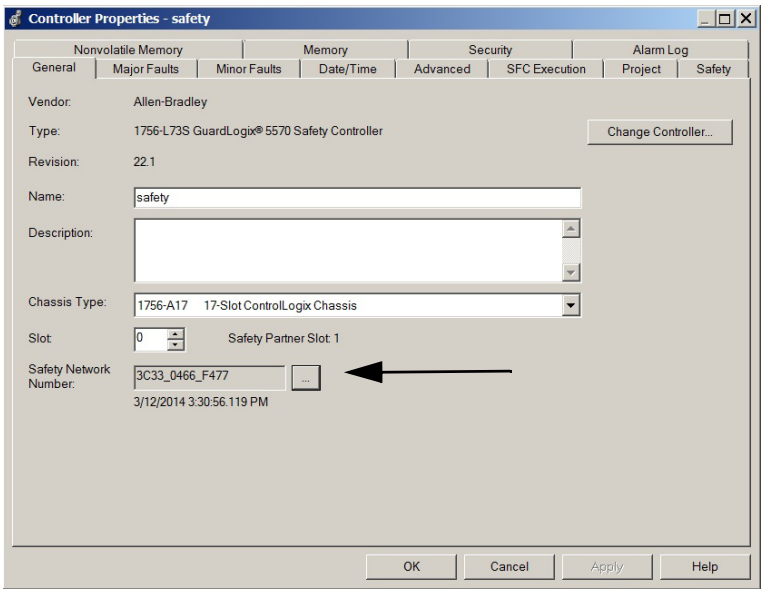
1. Fügen Sie die Producer-Steuerung dem E/A-Konfigurationsverzeichnis der Consumer-Steuerung hinzu.

HINWEIS Dieselbe produzierende Steuerung darf nur einmal im E/A-Konfigurationsverzeichnis der Steuerung angezeigt werden. Andernfalls tritt ein Verifizierungsfehler auf.

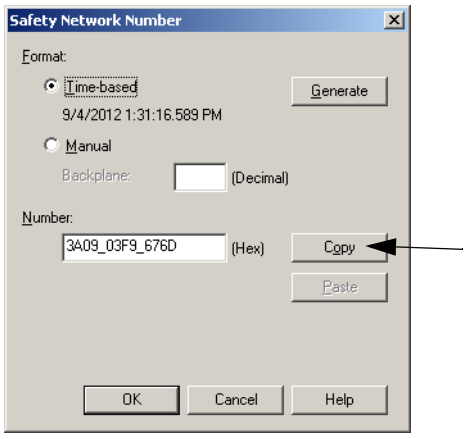


2. Klicken Sie im Steuerungsprojekt des Producers mit der rechten Maustaste auf die produzierende Steuerung und wählen Sie „Controller Properties“ (Steuerungseigenschaften) aus.

3. Durch Klicken auf die Schaltfläche ... wird das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) geöffnet.



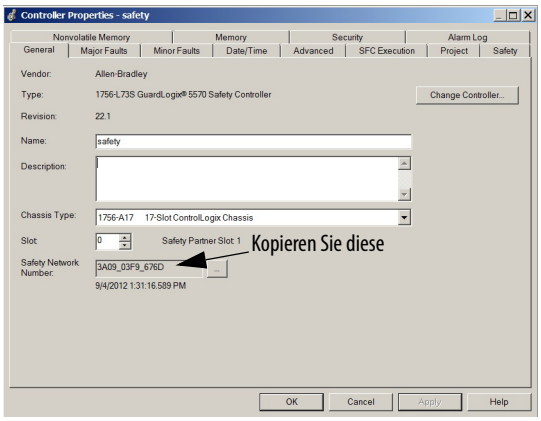
4. Kopieren Sie die SNN der Producer-Steuerung.



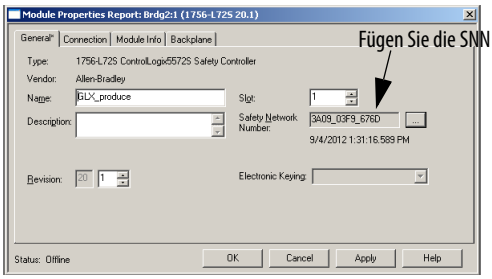
5. Klicken Sie im Steuerungsprojekt des Consumers mit der rechten Maustaste auf die produzierende Steuerung und wählen Sie „Module Properties“ (Moduleigenschaften) aus.
6. Durch Klicken auf die Schaltfläche ... wird das Dialogfeld „Safety Network Number“ (Sicherheitsnetzwerknummer) geöffnet.
7. Fügen Sie die SNN der Producer-Steuerung in das Feld für die SNN ein und klicken Sie auf „OK“.

   Die Sicherheitsnetzwerknummern stimmen überein.

Dialogfeld „Controller Properties“ (Steuerungseigenschaften) des



Dialogfeld „Module Properties“ (Moduleigenschaften) im Consu



Erstellen eines Sicherheits-Tags

Gehen Sie zum Erstellen eines Sicherheits-Tags wie folgt vor.

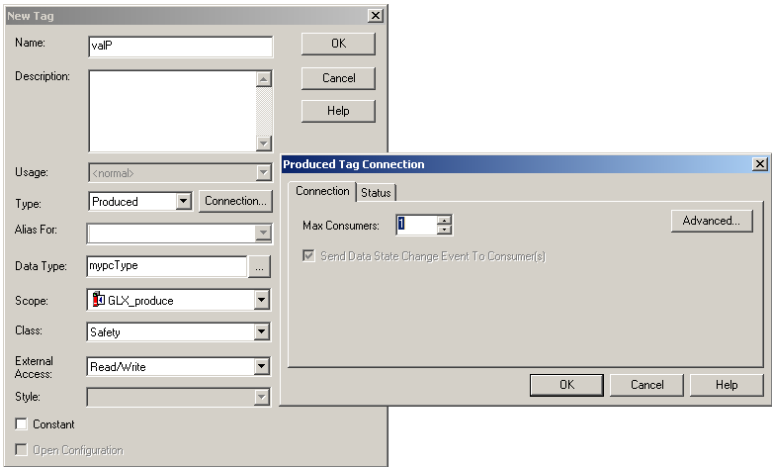
1. Erstellen Sie im Projekt der produzierenden Steuerung einen benutzerdefinierten Datentyp, der die Struktur der zu produzierenden Daten definiert.

   Vergewissern Sie sich, dass das erste Datenglied den Datentyp CONNECTION_STATUS aufweist.

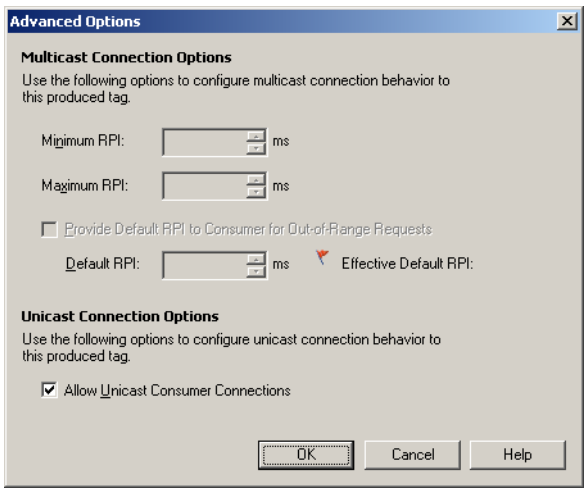
2. Klicken Sie mit der rechten Maustaste auf „Controller Tags“ (Steuerungs-Tags) und wählen Sie „New Tag“ (Neues Tag) aus.

3. Legen Sie als Typ „Produced“ (Produziert), für die Klasse „Safety“ (Sicherheit) und als Datentyp den in Schritt 1 erstellten benutzerdefinierten Datentyp fest.

4. Klicken Sie auf „Connection“ (Verbindung) und geben Sie die Anzahl der Steuerungen ein, die Daten konsumieren werden.



5. Klicken Sie auf „Advanced“ (Erweitert), wenn Sie den Verbindungstyp durch Deaktivierung von „Allow Unicast Consumer Connections“ (Unicast-Consumer-Verbindungen zulassen) ändern möchten.



6. Klicken Sie auf „OK“.

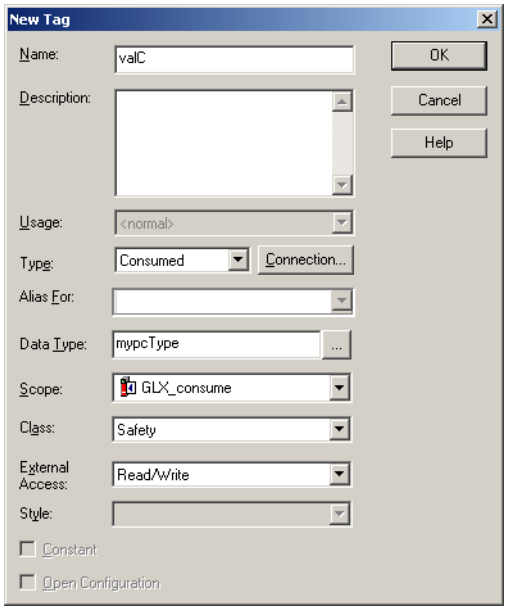
Konsumieren von Sicherheits-Tag-Daten

Gehen Sie wie folgt vor, um Daten zu konsumieren, die von einer anderen Steuerung produziert wurden.

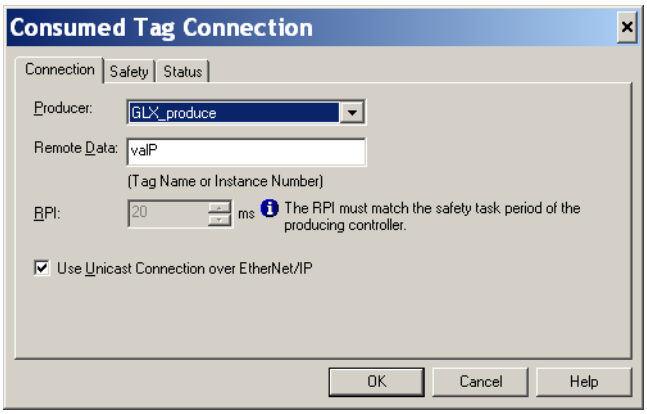
1. Erstellen Sie im Projekt der konsumierenden Steuerung einen benutzerdefinierten Datentyp, der mit dem im Producer-Projekt erstellten Datentyp identisch ist.

   HINWEIS Der benutzerdefinierte Datentyp kann aus dem Producer-Projekt kopiert und in das Consumer-Projekt eingefügt werden.

2. Klicken Sie mit der rechten Maustaste auf „Controller Tags“ (Steuerungs-Tags) und wählen Sie „New Tag“ (Neues Tag) aus.
3. Legen Sie als Typ „Consumed“ (Konsumiert), für die Klasse „Safety“ (Sicherheit) und als Datentyp den in Schritt 1 erstellten benutzerdefinierten Datentyp fest.



4. Klicken Sie auf „Connection“ (Verbindung), um das Dialogfeld „Consumed Tag Connection“ (Verbindung konsumiertes Tag) zu öffnen.

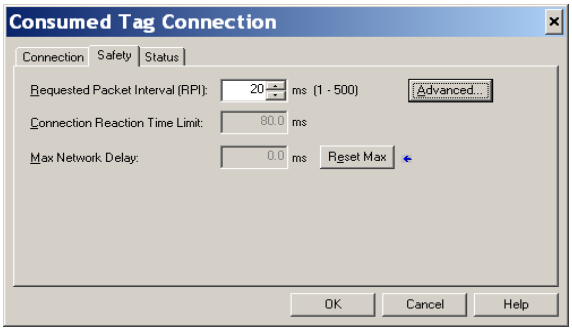


5. Wählen Sie Menü „Producer“ die Steuerung aus, die die Daten erzeugt.
6. Geben Sie im Feld „Remote Data“ den Namen des erzeugten Tags ein.

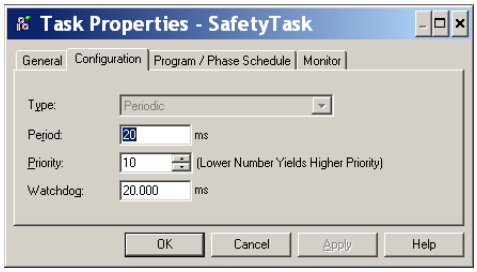
7. Klicken Sie auf die Registerkarte „Safety“ (Sicherheit).
8. Geben Sie im Feld „Requested Packet Interval“ (Angefordertes Paketintervall (RPI)) das angeforderte Paketintervall für die Verbindung in Einheiten von 1 ms ein.

   Der Standardwert ist 20 ms.

Consumer-Projekt



Producer-Projekt

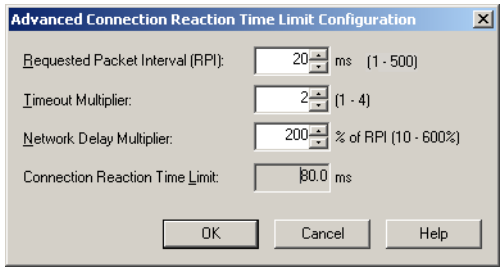


Das angeforderte Paketintervall (RPI) spezifiziert den Zeitraum, in dem die Daten über eine Verbindung aktualisiert werden. Das RPI des konsumierten Sicherheits-Tags muss der Sicherheits-Task-Zeitspanne des produzierenden Sicherheitsprojekts entsprechen.

Die Reaktionszeitgrenze der Verbindung ist das maximale Alter der Sicherheitspakete auf der zugehörigen Verbindung. Für einfache Zeitmessungsbedingungen kann eine zweckmäßige Reaktionszeitgrenze der Verbindung durch Einstellen des RPI erreicht werden.

Die maximale Netzwerkverzögerung ist die beobachtete maximale Transportverzögerung vom Zeitpunkt der Datenerzeugung bis zum Zeitpunkt des Datenempfangs. Klicken Sie im Online-Modus auf „Reset Max“ (Zurücksetzen Max), um die maximale Netzwerkverzögerung zurückzusetzen.

9. Wenn die Reaktionszeitgrenze der Verbindung übernommen werden soll, klicken Sie auf „OK“. Wenn Sie weitere Anforderungen haben, klicken Sie auf „Advanced“ (Erweitert), um die erweiterten Parameter für die Reaktionszeitgrenze der Verbindung aufzurufen.



Der Timeout-Multiplikator bestimmt die Anzahl der RPIs, die auf ein Paket gewartet wird, bevor ein Verbindungs-Timeout erfolgt.

Der Netzwerkverzögerungs-Multiplikator definiert die Nachrichtentransportzeit, die durch das Sicherheitsprotokoll CIP Safety erzwungen wird. Er spezifiziert die Verzögerung durch die Übertragung vom Producer zum Consumer und zurück und die Rückbestätigung zum Producer. Sie können den Netzwerkverzögerungs-Multiplikator verwenden, um die Reaktionszeitgrenze der Verbindung zu erhöhen oder zu verringern.

Tabelle 31 – Weitere Informationen

Quelle	Beschreibung
Seite 72 bis 73	Enthält weitere Informationen zur Einstellung des angeforderten Paketintervalls (RPI) und dazu, wie sich maximale Netzwerkverzögerung, Timeout-Multiplikator und Netzwerkverzögerungs-Multiplikatoren auf die Reaktionszeitgrenze der Verbindung auswirken
Kapitel 9	Enthält Informationen zum vordefinierten Datentyp CONNECTION_STATUS (VERBINDUNGSSTATUS)
Logix5000 Controllers Produced and Consumed Tags Programming Manual, Publikation 1756-PM011	Stellt ausführliche Informationen zum Verwenden produzierter und konsumierter Tags zur Verfügung

Zuordnen von Sicherheits-Tags

Auf Steuerungsbereichs-Standard-Tags kann nicht direkt durch eine Sicherheitsroutine zugegriffen werden. Damit in Sicherheits-Task-Routinen Standard-Tag-Daten verwendet werden können, stellen die GuardLogix-Steuerungen eine Zuordnungsfunktion (Mapping) für Sicherheits-Tags zur Verfügung, mit der Standard-Tag-Werte in den Sicherheits-Task-Speicher kopiert werden können.

Einschränkungen

Das Zuordnen von Sicherheits-Tags unterliegt den folgenden Einschränkungen:

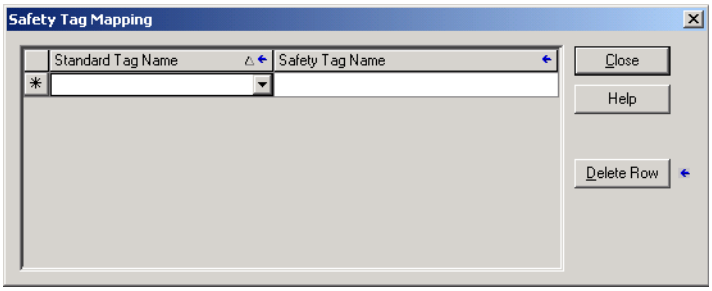
- Beim Sicherheits-Tag- und Standard-Tag-Paar muss es sich um Steuerungsbereichs-Tags handeln.
- Die Datentypen des Sicherheits- und Standard-Tag-Paars müssen übereinstimmen.
- Alias-Tags sind nicht zulässig.
- Die Zuordnung muss für die gesamte Tag-Ebene erfolgen. Zum Beispiel, myTimer.pre ist nicht zulässig, wenn myTimer ein TIMER-Tag ist.
- Ein Zuordnungspaar entspricht einem Standard-Tag, das einem Sicherheits-Tag zugeordnet ist.
- Sie können ein Standard-Tag keinem Sicherheits-Tag zuordnen, das als Konstante gekennzeichnet wurde.
- Die Tag-Zuordnung kann nicht geändert werden, wenn:
  - das Projekt sicherheitsgesperrt ist.
  - eine Sicherheits-Task-Signatur vorliegt.
  - der Schlüsselschalter sich in der RUN-Position befindet.
  - ein nicht korrigierbarer Sicherheitsfehler vorliegt.
  - eine ungültige Partnerschaft zwischen der Primärsteuerung und dem Sicherheitspartner besteht.

ACHTUNG: Beim Verwenden von Standarddaten in einer Sicherheitsroutine müssen Sie sicherstellen, dass die Daten angemessen genutzt werden. Wenn Sie Standarddaten in einem Sicherheits-Tag verwenden, werden diese nicht zu Sicherheitsdaten. Sie dürfen einen SIL 3/PLe-Sicherheitsausgang nicht direkt mit Standard-Tag-Daten steuern.

Weitere Informationen finden Sie in der Publikation 1756-RM099, Steuerungssysteme GuardLogix 5570 – Sicherheitsreferenzhandbuch.

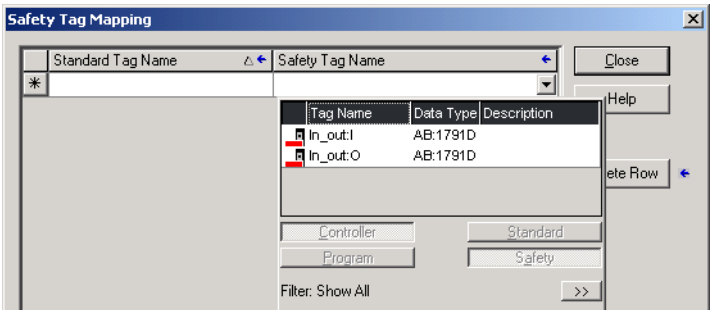
Erstellen von Tag-Zuordnungspaaren

1. Wählen Sie im Menü „Logic“ (Logik) die Option „Map Safety Tags“ (Sicherheits-Tags zuordnen) aus, um das Dialogfeld „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) zu öffnen.



2. Fügen Sie ein bestehendes Tag in die Spalte „Standard Tag Name“ (Standard-Tag-Name) oder die Spalte „Safety Tag Name“ (Sicherheits-Tag-Name) ein, indem Sie den Tag-Namen in die Zelle eingeben oder ein Tag aus dem Pulldown-Menü auswählen.

   Klicken Sie auf den Pfeil, um ein Dialogfeld mit einer gefilterten Tag-Suche aufzurufen. Wenn Sie sich in der Spalte „Standard Tag Name“ (Standard-Tag-Name) befinden, zeigt der Browser nur die Steuerungsbereichs-Standard-Tags an. Wenn Sie sich in der „Spalte Safety Tag Name“ (Sicherheits-Tag-Name) befinden, zeigt der Browser die Steuerungsbereichs-Sicherheits-Tags an.



3. Fügen Sie ein neues Tag in die Spalte „Standard Tag Name“ (Standard-Tag-Name) oder die Spalte „Safety Tag Name“ (Sicherheits-Tag-Name) ein, indem Sie mit der rechten Maustaste in die leere Zelle klicken, „New Tag“ (Neues Tag) auswählen und den Tag-Namen in die Zelle eingeben.
4. Klicken Sie mit der rechten Maustaste in die Zelle und wählen Sie „New ‚tagname‘“, wobei ‚tagname‘ der Text ist, den Sie in die Zelle eingegeben haben.

Überwachen des Tag-Zuordnungsstatus

Die äußerste linke Spalte des Dialogfelds „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) zeigt den Status des zugeordneten Paars an.

Tabelle 32 – Symbole zum Tag-Zuordnungsstatus

Zelleninhalte	Beschreibung
leer	Die Tag-Zuordnung ist gültig.
	Im Offline-Modus zeigt das Symbol X an, dass die Tag-Zuordnung ungültig ist. Sie können in eine andere Zeile wechseln oder das Dialogfeld „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) schließen.(1) Im Online-Modus hat eine ungültige Tag-Zuordnung eine Fehlermeldung zur Folge, die erläutert, warum die Zuordnung ungültig ist. Sie können nicht in eine andere Zeile wechseln oder das Dialogfeld „Safety Tag Mapping“ (Zuordnung von Sicherheits-Tags) schließen, wenn ein Tag-Zuordnungsfehler vorliegt.
	Zeigt die Zeile an, die momentan aktiv ist.
	Steht für die Zeile „Create New Mapped Tag“ (Neues zugeordnetes Tag erstellen).
	Steht für eine ausstehende Änderung.

(1) Die Tag-Zuordnung wird auch während der Projektverifizierung überprüft. Eine ungültige Tag-Zuordnung resultiert in einem Projektverifizierungsfehler.

Weitere Informationen enthält der Abschnitt zu den Einschränkungen bei der Zuordnung von Tags auf Seite 104.

Schutz von Sicherheitsanwendungen

Sie können Ihr Anwendungsprogramm vor unbefugten Änderungen schützen, wenn Sie für die Steuerung eine Sicherheitssperre aktivieren und die Sicherheits-Task-Signatur erstellen und speichern.

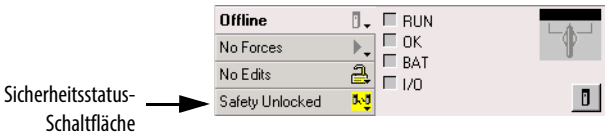
Sicherheitssperre der Steuerung

Die GuardLogix-Steuerung kann sicherheitsgesperrt werden, um sicherheitsbezogene Steuerungskomponenten vor Änderungen zu schützen. Die Funktion für die Sicherheitssperre gilt nur für Sicherheitskomponenten wie z. B. die Sicherheits-Task, Sicherheitsprogramme, Sicherheitsroutinen, Sicherheits-Add-On-Befehle, Sicherheits-Tags, Sicherheits-E/A und die Sicherheits-Task-Signatur.

Die nachfolgenden Aktionen sind im Sicherheitsteil der Anwendung erlaubt, wenn die Steuerung sicherheitsgesperrt ist:

- Online-/Offline-Programmierung oder -Bearbeitung (einschließlich der Sicherheits-Add-On-Befehle)
- Forcieren der Sicherheits-E/A
- Ändern des gesperrten Zustands von Sicherheits-E/A oder produzierten Verbindungen
- Manipulation von Sicherheitsdaten (außer durch Sicherheitsroutinenlogik)
- Erstellen oder Löschen der Sicherheits-Task-Signatur

HINWEIS Der Text der Sicherheitsstatus-Schaltfläche der Online-Leiste zeigt den Status der Sicherheitssperre an.



Auf der Anwendungsleiste sind auch die folgenden Symbole abgebildet, die den Status der Sicherheitssperre der Sicherheitssteuerung anzeigen.

- = Steuerung sicherheitsgesperrt
- = Steuerung sicherheitsentsperrt

Sie können das Steuerungsprojekt sicherheitssperren, und zwar unabhängig davon, ob Sie online oder offline sind, und unabhängig davon, ob Sie die Originalquelle des Programms haben oder nicht. Es dürfen allerdings keine Sicherheits-Force-Zustände oder ausstehenden Online-Sicherheitsbearbeitungen vorhanden sein.

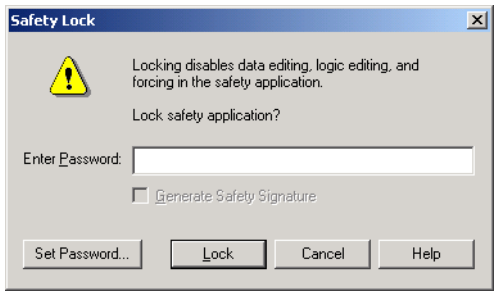
Der sicherheitsgesperrte bzw. sicherheitsentsperrte Zustand kann nicht geändert werden, wenn sich der Schlüsselschalter in der RUN-Position befindet.

HINWEIS Das Aktivieren oder Deaktivieren der Sicherheitssperre wird im Steuerungsprotokoll aufgezeichnet.

Weitere Informationen zum Zugriff auf das Steuerungsprotokoll finden Sie in der Publikation 1756-PM015, Logix5000 Controllers Controller Information and Status Programming Manual.

Sie können über die Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) oder durch Auswählen von „Tools>Safety>Safety Lock/Unlock“ (Tools>Sicherheit> Sicherheitssperrung/-entsperrung) die Sicherheitssperre für die Steuerung aktivieren und deaktivieren.

Abbildung 27 – Aktivieren der Sicherheitssperre der Steuerung



Wenn Sie die Funktion der Sicherheitssperre mit einem Kennwort schützen wollen, müssen Sie dieses in das Feld „Enter Password“ (Kennwort eingeben) eingeben. Andernfalls klicken Sie auf „Lock“ (Sperren).

Sie können das Kennwort auch über das Dialogfeld „Safety Lock“ (Sicherheitssperre) einstellen oder ändern. Siehe Seite 47.

Die in diesem Abschnitt beschriebene Funktion für die Sicherheitssperre und die Standardsicherheitsmaßnahmen in der Anwendung Logix Designer gelten für GuardLogix-Steuerungsprojekte.

Weitere Informationen zu den Sicherheitsfunktionen von Logix Designer finden Sie in der Publikation 1756-PM016, Logix5000-Steuerungen – Sicherheit – Programmierhandbuch.

Erstellen einer Sicherheits-Task-Signatur

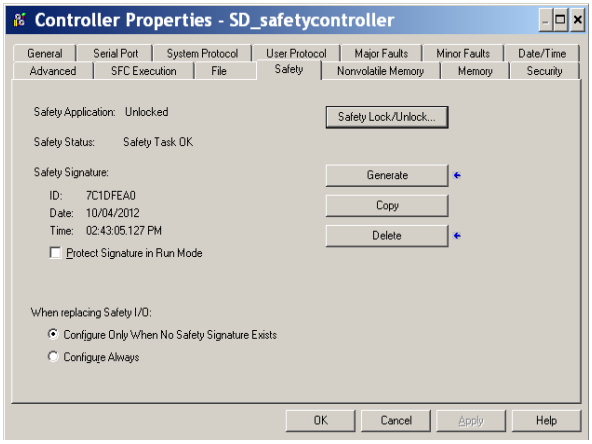
Vor der Verifizierungsprüfung müssen Sie die Sicherheits-Task-Signatur erstellen. Sie können diese Sicherheits-Task-Signatur nur erstellen, wenn die GuardLogix-Steuerung online, im Programm-Modus und sicherheitsentsperrt ist und keine Sicherheits-Force-Zustände, ausstehenden Online-Sicherheitsbearbeitungen oder Sicherheitsfehler vorliegen. Der Sicherheitsstatus muss „Safety Task OK“ (Sicherheits-Task OK) lauten.

Darüber hinaus können Sie keine Sicherheits-Task-Signatur erstellen, wenn sich die Steuerung im Run-Modus bei aktiviertem Run-Modus-Schutz befindet.

HINWEIS Sie können den Sicherheitsstatus über die Sicherheitsstatus-Schaltfläche auf der Online-Leiste (siehe Seite 126) oder auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften), wie auf Seite 108 dargestellt, einsehen.

Sie können die Sicherheits-Task-Signatur auf der Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) durch Klicken auf die Schaltfläche „Generate“ (Generieren) erstellen. Alternativ dazu können Sie „Tools>Safety>Generate Signature“ (Tools>Sicherheit>Signatur generieren) auswählen.

Abbildung 28 – Registerkarte „Sicherheit“



Gegebenenfalls werden Sie aufgefordert, eine bereits bestehende Signatur zu überschreiben.

HINWEIS Das Erstellen und Löschen der Sicherheits-Task-Signatur wird im Steuerungsprotokoll aufgezeichnet.

Weitere Informationen zum Zugriff auf das Steuerungsprotokoll finden Sie in der Publikation 1756-PM015, Logix5000 Controllers Controller Information and Status Programming Manual.

Wenn eine Sicherheits-Task-Signatur vorhanden ist, sind die nachfolgenden Aktionen im Sicherheitsteil der Anwendung nicht zulässig.

- Online-/Offline-Programmierung oder -Bearbeitung (einschließlich der Sicherheits-Add-On-Befehle)
- Forcieren der Sicherheits-E/A
- Ändern des gesperrten Zustands von Sicherheits-E/A oder Producer-Steuerungen
- Manipulation von Sicherheitsdaten (außer durch Sicherheitsroutinenlogik)

Kopieren der Sicherheits-Task-Signatur

Über die Schaltfläche „Copy“ (Kopieren) können Sie ein Protokoll der Sicherheits-Task-Signatur zur Verwendung bei Dokumentation, Vergleich und Validierung des Sicherheitsprojekts erstellen. Klicken Sie auf „Copy“ (Kopieren), um die ID-, Datum- und Zeitkomponenten in die Windows-Zwischenablage zu kopieren.

Löschen der Sicherheits-Task-Signatur

Klicken Sie auf „Delete“ (Löschen), um die Sicherheits-Task-Signatur zu löschen. Die Sicherheits-Task-Signatur kann in folgenden Fällen nicht gelöscht werden:

- wenn die Steuerung sicherheitsgesperrt ist.
- wenn sich die Steuerung im Run-Modus befindet und der Schlüsselschalter auf RUN steht.
- wenn sich die Steuerung im Run-Modus oder Remote Run-Modus befindet und der Run-Modus-Schutz aktiviert ist.

ACHTUNG: Wenn Sie die Sicherheits-Task-Signatur löschen, müssen Sie Ihr System erneut testen und überprüfen, ob die Anforderungen von SIL 3/PLe weiterhin erfüllt werden.

Weitere Informationen zu den Anforderungen für SIL 3/PLe finden Sie in der Publikation 1756-RM099, Steuerungssysteme GuardLogix 5570 – Sicherheitsreferenzhandbuch.

Einschränkungen bei der Programmierung

Die Verfügbarkeit einiger Menüpunkte und Funktionsmerkmale (z. B. Ausschneiden, Einfügen, Löschen, Suchen und Ersetzen) wird zum Schutz der Sicherheitskomponenten vor Änderung durch die Anwendung Logix Designer eingeschränkt, wenn:

- wenn die Steuerung sicherheitsgesperrt ist.
- eine Sicherheits-Task-Signatur vorliegt.
- Sicherheitsfehler vorhanden sind.
- der Sicherheitsstatus wie folgt lautet:
  - Partner fehlt.
  - Partner nicht verfügbar.
  - Hardware inkompatibel.
  - Firmware inkompatibel.

Trifft auch nur eine dieser Bedingungen zu, ist Folgendes nicht möglich:

- Erstellen oder Ändern von Sicherheitsobjekten, wie z. B. Sicherheitsprogrammen, Sicherheitsroutinen, Sicherheits-Tags, Sicherheits-Add-On-Befehlen und Sicherheits-E/A-Geräten.

  WICHTIG Die Abtastzeiten der Sicherheits-Task und Sicherheitsprogramme können im Online-Modus zurückgesetzt werden.

- Anwendung von Force-Zuständen auf Sicherheits-Tags.
- Erstellung neuer Sicherheits-Tag-Zuordnungen.
- Änderung oder Löschung von Tag-Zuordnungen.
- Änderung oder Löschung benutzerdefinierter Datentypen, die von Sicherheits-Tags verwendet werden.
- Änderung des Steuerungsnamens, der Beschreibung, des Chassistyps, des Steckplatzes und der Sicherheitsnetzwerknummer.
- Änderung oder Löschung der Sicherheits-Task-Signatur im sicherheitsgesperrten Zustand.

Schalten der Steuerung in den Online-Modus

Thema	Seite
Verbinden der Steuerung mit dem Netzwerk	111
Faktoren, die das Schalten in den Online-Modus beeinflussen	112
Herunterladen	115
Hochladen	116
Schalten in den Online-Modus	117

Verbinden der Steuerung mit dem Netzwerk

Wenn noch nicht geschehen, verbinden Sie die Steuerung mit dem Netzwerk.

Tabelle 33 – Kommunikationsanschlüsse

Für diesen Anschlusstyp	Zu verwendende Software	Siehe
USB	USB 2.0-Kabel	Herstellen einer Kommunikationsverbindung auf Seite 33
EtherNet/IP	EtherNet/IP-Gerät in einem unbelegten Steckplatz im selben Chassis wie die Steuerung	Verbinden Ihres EtherNet/IP-Geräts mit dem Computer auf Seite 111
DeviceNet	Modul 1756-DNB in einem unbelegten Steckplatz im selben Chassis wie die Steuerung	Verbinden Ihres ControlNet-Kommunikationsmoduls oder Ihres DeviceNet-Scanners mit Ihrem Computer auf Seite 112
ControlNet	Modul 1756-CN2 in einem unbelegten Steckplatz im selben Chassis wie die Steuerung	

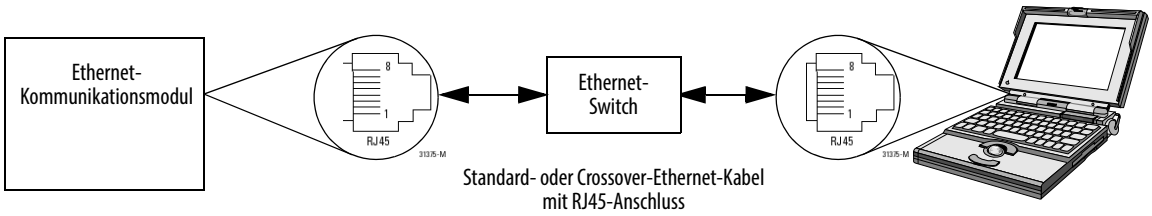
Verbinden Ihres EtherNet/IP-Geräts mit dem Computer

WARNUNG: Wenn Sie das Verbindungskabel anschließen oder abziehen, solange die Stromversorgung dieses Moduls oder eines anderen Geräts im Netzwerk eingeschaltet ist, kann ein elektrischer Lichtbogen erzeugt werden. In Gefahrenbereichen kann dadurch eine Explosion hervorgerufen werden.

Sorgen Sie dafür, dass die Stromversorgung unterbrochen ist und dass Sie nicht in einem explosionsgefährdeten Bereich arbeiten.

Verbinden Sie Ihr EtherNet/IP-Gerät und den Computer mit einem Ethernet-Kabel.

Abbildung 29 – Ethernet-Anschlüsse



Verbinden Ihres ControlNet-Kommunikationsmoduls oder Ihres DeviceNet-Scanners mit Ihrem Computer

Zugriff auf das ControlNet- oder DeviceNet-Netzwerk erhalten Sie, indem Sie entweder:

- eine direkte Verbindung zum Netzwerk herstellen oder
- eine Verbindung zu einem seriellen oder einem EtherNet/IP-Netzwerk herstellen und zum gewünschten Netzwerk navigieren (Bridge). Dies verlangt keine zusätzliche Programmierung.

Konfigurieren eines EtherNet/IP-, ControlNet- oder DeviceNet-Treibers

Informationen zum Konfigurieren eines Treibers finden Sie in der entsprechenden Publikation.

- EtherNet/IP-Module in Logix5000-Steuerungssystemen – Benutzerhandbuch, Publikation ENET-UM001
- ControlNet Modules in Logix5000 Control Systems User Manual, Publikation CNET-UM001
- DeviceNet Modules in Logix5000 Control Systems, Publikation DNET-UM004

Faktoren, die das Schalten in den Online-Modus beeinflussen

Die Anwendung Logix Designer legt fest, ob Sie mit einer Zielsteuerung abhängig davon in den Online-Modus schalten können, ob das Offline-Projekt neu ist oder ob Änderungen im Offline-Projekt vorgenommen wurden. Wenn das Projekt neu ist, müssen Sie zuerst das Projekt auf die Steuerung herunterladen. Wenn am Projekt Änderungen vorgenommen wurden, werden Sie zum Hoch- oder Herunterladen aufgefordert. Falls keine Änderungen vorgenommen wurden, können Sie in den Online-Modus schalten, um die Ausführung des Projekts zu überwachen.

Diese Prozesse werden von verschiedenen Faktoren beeinflusst, so z. B. von der Funktion „Project to Controller Match“ (Übereinstimmung zwischen Projekt und Steuerung), vom Sicherheitsstatus und von den Sicherheitsfehlern, ob eine Sicherheits-Task-Signatur vorliegt oder nicht sowie vom Status der Sicherheitssperrung/-entsperrung des Projekts und der Steuerung.

Übereinstimmung zwischen Projekt und Steuerung

Die Funktion „Project to Controller Match“ (Übereinstimmung zwischen Projekt und Steuerung) hat Auswirkungen auf das Herunterladen, das Hochladen und auf die Verfahren zum Online-Schalten von Standard- und Sicherheitsprojekten.

Ist die Funktion „Project to Controller Match“ (Übereinstimmung zwischen Projekt und Steuerung) im Offline-Projekt aktiviert, vergleicht die Anwendung Logix Designer die Seriennummer der Steuerung im Offline-Projekt mit der Seriennummer der angeschlossenen Steuerung. Falls diese nicht übereinstimmen, müssen Sie entweder das Hoch- bzw. Herunterladen abbrechen, eine Verbindung zur richtigen Steuerung herstellen oder bestätigen, dass Sie eine Verbindung zur richtigen Steuerung hergestellt haben. In diesem Fall wird die Seriennummer im Projekt aktualisiert, damit sie mit der Zielsteuerung übereinstimmt.

Firmware-Versionsübereinstimmung

Die Firmware-Versionsübereinstimmung hat Auswirkungen auf den Download-Prozess. Falls die Version der Steuerung nicht mit der Version des Projekts übereinstimmt, werden Sie aufgefordert, die Firmware der Steuerung zu aktualisieren. Die Anwendung Logix Designer ermöglicht Ihnen das Aktualisieren der Firmware als Teil der Download-Sequenz.

WICHTIG	Um die Firmware der Steuerung zu aktualisieren, müssen Sie zuerst ein Firmware-Upgrade-Kit installieren. Ein Upgrade-Kit wird auf einer Ergänzungs-DVD zusammen mit der Studio 5000-Umgebung geliefert.

HINWEIS	Für ein Firmware-Upgrade können Sie auch in der Anwendung Logix Designer im Menü „Tools“ die Option „ControlFLASH“ (Flash-Speicher der Steuerung) auswählen.

Sicherheitsstatus/-fehler

Das Hochladen der Programmlogik und das Online-Schalten sind, unabhängig vom Sicherheitsstatus, immer zulässig. Sicherheitsstatus und -fehler wirken sich nur auf das Herunterladen aus.

Sie können den Sicherheitsstatus über die Registerkarte „Safety“ (Sicherheit) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) einsehen.

Sicherheits-Task-Signatur sowie sicherheitsgesperrter und -entsperrter Zustand

Das Vorliegen einer Sicherheits-Task-Signatur und des sicherheitsgesperrten oder -entsperrten Zustands der Steuerung wirken sich auf das Hoch- und Herunterladen aus.

Beim Upload

Wenn die Steuerung über eine Sicherheits-Task-Signatur verfügt, werden die Sicherheits-Task-Signatur und der Sperrzustand der Sicherheits-Task mit dem Projekt hochgeladen. Wenn das Projekt in der Steuerung zum Beispiel sicherheitsentsperrt war, bleibt es nach dem Hochladen sicherheitsentsperrt, selbst wenn das Offline-Projekt vor dem Hochladen gesperrt war.

Nach dem Hochladen stimmt die Sicherheits-Task-Signatur im Offline-Projekt mit der Sicherheits-Task-Signatur der Steuerung überein.

Beim Herunterladen

Das Vorhandensein einer Sicherheits-Task-Signatur und des sicherheitsgesperrten Zustands der Steuerung bestimmt, ob das Herunterladen fortgesetzt werden kann.

Tabelle 34 – Auswirkung von Sicherheitssperre und Sicherheits-Task-Signatur auf das Herunterladen

Sicherheitssperrzustand	Status der Sicherheits-Task-Signatur	Download-Funktionalität
Steuerung sicherheitsentsperrt	Die Sicherheits-Task-Signatur im Offline-Projekt stimmt mit der Sicherheits-Task-Signatur der Steuerung überein.	Alle Standardprojektkomponenten werden heruntergeladen. Sicherheits-Tags werden auf die zum Zeitpunkt der Signaturerstellung für die Sicherheits-Task eingestellten Werte zurückgesetzt. Die Sicherheits-Task wird nicht heruntergeladen. Der Status der Sicherheitssperre stimmt mit dem Status im Offline-Projekt überein.
	Die Signaturen der Sicherheits-Tasks stimmen nicht überein.	Wenn in der Steuerung eine Sicherheits-Task-Signatur vorlag, wird diese automatisch gelöscht und das gesamte Projekt wird heruntergeladen. Der Status der Sicherheitssperre stimmt mit dem Status im Offline-Projekt überein.
Steuerung sicherheitsgesperrt	Die Signaturen der Sicherheits-Tasks stimmen überein.	Wenn das Offline-Projekt und die Steuerung sicherheitsgesperrt sind, werden alle Standardprojektkomponenten heruntergeladen und die Sicherheits-Task wird erneut mit den Werten initialisiert, die beim Erstellen der Sicherheits-Task-Signatur vorlagen. Ist das Offline-Projekt nicht sicherheitsgesperrt, die Steuerung jedoch schon, wird das Herunterladen blockiert und erst wieder nach Entsperrung der Steuerung fortgesetzt.
	Die Signaturen der Sicherheits-Tasks stimmen nicht überein.	Sie müssen zur Fortsetzung des Download-Vorgangs die Steuerung sicherheitsentsperren. Wenn in der Steuerung eine Sicherheits-Task-Signatur vorlag, wird diese automatisch gelöscht und das gesamte Projekt wird heruntergeladen. Der Status der Sicherheitssperre stimmt mit dem Status im Offline-Projekt überein.

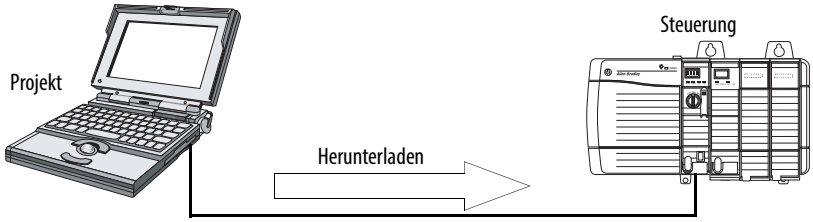
WICHTIG Unterscheidet sich während des Herunterladens auf eine sicherheitsentsperrte Steuerung die Firmware in der Steuerung von der im Offline-Projekt, gehen Sie auf eine der folgenden Weisen vor:

- Aktualisieren Sie die Steuerung, so dass diese mit dem Offline-Projekt übereinstimmt. Nach Abschluss der Aktualisierung wird das gesamte Projekt heruntergeladen.
- Aktualisieren Sie das Projekt entsprechend der Steuerungsversion.

Wenn Sie das Projekt aktualisieren, wird die Sicherheits-Task gelöscht und das System muss erneut validiert werden.

Herunterladen

Gehen Sie wie folgt vor, um Ihr Projekt von Ihrem Computer auf Ihre Steuerung zu übertragen.



1. Stellen Sie den Schlüsselschalter der Steuerung auf REM.
2. Öffnen Sie das Steuerungsprojekt, das Sie herunterladen möchten.
3. Legen Sie den Pfad zur Steuerung fest.
   a. Klicken Sie auf „Who Active“ (Aktive Geräte) .
   b. Wählen Sie die Steuerung aus.
   Klicken Sie zum Öffnen einer Ebene auf das Pluszeichen (+). Ist bereits eine Steuerung ausgewählt, stellen Sie sicher, dass es sich um die richtige Steuerung handelt.
4. Klicken Sie auf „Download“ (Herunterladen).

   Die Anwendung Logix Designer vergleicht die folgenden Informationen im Offline-Projekt und in der Steuerung.
   - Seriennummer der Steuerung (wenn die Option „Übereinstimmung zwischen Projekt und Steuerung“ ausgewählt ist)
   - Haupt- und Nebenversionen der Firmware
   - Sicherheitsstatus
   - Sicherheits-Task-Signatur (falls vorhanden)
   - Sicherheitssperrzustand
5. Befolgen Sie die Anweisungen in dieser Tabelle, um den Download-Vorgang basierend auf der Antwort der Anwendung Logix Designer abzuschließen.

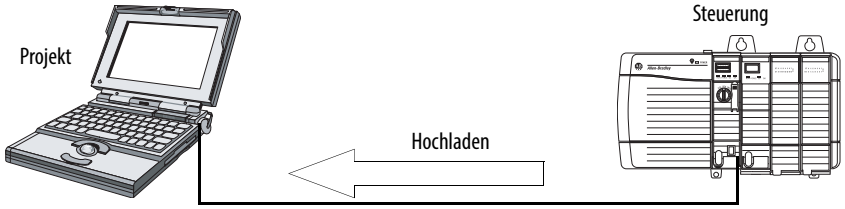
Zeigt die Software Folgendes an	Dann
Download auf die Steuerung.	Wählen Sie „Download“ (Herunterladen) aus. Das Projekt wird auf die Steuerung heruntergeladen und wechselt in den Online-Modus.
Download auf die Steuerung nicht möglich. Fehlende Übereinstimmung zwischen der Seriennummer des Offline-Projekts und der Seriennummer der Steuerung. Die ausgewählte Steuerung könnte die falsche Steuerung sein.	Schließen Sie die korrekte Steuerung an oder überprüfen Sie, dass es sich um die korrekte Steuerung handelt. Aktivieren Sie sodann das Optionsfeld „Update project serial number“ (Seriennummer des Projekts aktualisieren) und setzen Sie den Download-Vorgang fort. Die Seriennummer des Projekts wird entsprechend der Seriennummer der Steuerung geändert.
Download auf die Steuerung nicht möglich. Die Hauptversion des Offline-Projekts und die Firmware der Steuerung sind nicht kompatibel.	Wählen Sie „Update Firmware“ (Firmware aktualisieren). Klicken Sie nach Auswahl der erforderlichen Version auf „Update“ (Aktualisieren). Klicken Sie auf „Yes“ (Ja), um Ihre Auswahl zu bestätigen.
Download auf die Steuerung nicht möglich. Sicherheitspartner fehlt oder ist nicht verfügbar.	Download-Vorgang abbrechen. Installieren Sie einen kompatiblen Sicherheitspartner, bevor Sie einen erneuten Download-Versuch starten.
Download auf die Steuerung nicht möglich. Die Firmware-Version des Sicherheitspartners ist mit der Primärsteuerung nicht kompatibel.	Aktualisieren Sie die Firmware-Version des Sicherheitspartners. Wählen Sie „Update Firmware“ (Firmware aktualisieren). Klicken Sie nach Auswahl der erforderlichen Version auf „Update“ (Aktualisieren). Klicken Sie auf „Yes“ (Ja), um Ihre Auswahl zu bestätigen.
Download auf die Steuerung nicht möglich. Die Sicherheitspartnerschaft wurde nicht hergestellt.	Brechen Sie den Download-Vorgang ab und starten Sie einen erneuten Versuch.
Download auf die Steuerung nicht möglich. Die inkompatible Sicherheits-Task-Signatur kann nicht gelöscht werden, solange das Projekt sicherheitsgesperrt ist.	Brechen Sie den Download-Vorgang ab. Zum Herunterladen des Projekts müssen Sie die Sicherheitssperre des Offline-Projekts deaktivieren, die Sicherheits-Task-Signatur löschen und das Projekt herunterladen. **WICHTIG:** Das Sicherheitssystem erfordert eine erneute Validierung.

Zeigt die Software Folgendes an	Dann
Herunterladen unter Beibehaltung der Sicherheits-Task-Signatur nicht möglich. Die Nebenversion der Steuerungs-Firmware ist mit der Sicherheits-Task-Signatur im Offline-Projekt nicht kompatibel.	• Ist die Nebenversion der Steuerungs-Firmware nicht kompatibel, aktualisieren Sie zur Beibehaltung der Sicherheits-Task-Signatur die Firmware-Version in der Steuerung, sodass sie exakt mit dem Offline-Projekt übereinstimmt. Laden Sie dann das Offline-Projekt herunter. • Um trotz der Inkompatibilität der Sicherheits-Task-Signatur mit dem Herunterladen fortzufahren, klicken Sie auf „Download“ (Herunterladen). Die Sicherheits-Task-Signatur wird gelöscht. **WICHTIG:** Das Sicherheitssystem erfordert eine erneute Validierung.
Download auf die Steuerung nicht möglich. Die Steuerung ist gesperrt. Die Signaturen der Sicherheits-Tasks von Steuerung und Offline-Projekt stimmen nicht überein.	Wählen Sie „Unlock“ (Entsperren). Das Dialogfeld „Safety Unlock for Download“ (Sicherheitsentsperrung für Herunterladen) wird angezeigt. Bestätigen Sie nach Auswahl des Optionsfelds „Delete Signature“ (Signatur löschen) und „Unlock“ (Entsperren) Ihre Eingabe mit „Yes“ (Ja).
In der Sicherheitssteuerung tritt ein nicht korrigierbarer Sicherheitsfehler auf. Es wurde kein CST-Master (Master für koordinierte Systemzeit) festgelegt.	Wählen Sie „Enable Time Synchronization“ (Zeitsynchronisierung aktivieren) aus und klicken Sie zum Fortsetzen des Vorgangs auf „Download“ (Herunterladen).

Im Anschluss an das erfolgreiche Herunterladen stimmen der Sicherheitssperrzustand und die Sicherheits-Task-Signatur der Steuerung mit dem heruntergeladenen Projekt überein. Sicherheitsdaten werden mit den Werten initialisiert, die während der Erstellung der Sicherheits-Task-Signatur vorlagen.

Hochladen

Gehen Sie wie folgt vor, um ein Projekt aus der Steuerung auf Ihren Computer zu übertragen.



1. Legen Sie den Pfad zur Steuerung fest.
   a. Klicken Sie auf „Who Active“ (Aktive Geräte) .
   b. Wählen Sie die Steuerung aus.
   Klicken Sie zum Erweitern einer Ebene auf das Pluszeichen (+). Ist bereits eine Steuerung ausgewählt, stellen Sie sicher, dass es sich um die richtige Steuerung handelt.
2. Klicken Sie auf „Upload“ (Hochladen).
3. Falls die Projektdatei nicht vorhanden ist, wählen Sie „File>Select>Yes“ (Datei>Auswählen>Ja) aus.
4. Falls das Projekt bereits besteht, wählen Sie es aus.

   Ist die Überprüfung der Übereinstimmung zwischen Projekt und Steuerung aktiviert, überprüft die Anwendung Logix Designer, ob die Seriennummer des geöffneten Projekts und die Seriennummer der Steuerung übereinstimmen.

   Stimmen die Seriennummern nicht überein, können Sie:

   • den Upload-Vorgang abbrechen und eine Verbindung zu einer übereinstimmenden Steuerung herstellen. Starten Sie den Upload-Vorgang dann erneut.

- ein neues Projekt zum Hochladen auswählen oder ein anderes Projekt auswählen, indem Sie auf „Select File“ (Datei auswählen) klicken.
- die Seriennummer des Projekts aktualisieren, so dass sie mit der Steuerung übereinstimmt, indem Sie das Optionsfeld „Update Project Serial Number“ (Seriennummer des Projekts aktualisieren) auswählen und dann auf „Upload“ (Hochladen) klicken.

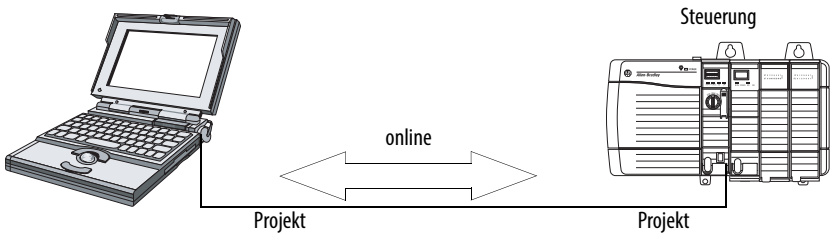
5. Die Anwendung Logix Designer prüft, ob das geöffnete Projekt mit dem Steuerungsprojekt übereinstimmt.
   a. Stimmen die Projekte nicht überein, müssen Sie eine übereinstimmende Datei auswählen oder den Upload-Vorgang abbrechen.
   b. Stimmen die Projekte überein, führt die Software eine Prüfung auf Änderungen im (geöffneten) Offline-Projekt durch.
6. Die Anwendung Logix Designer sucht nach Änderungen im Offline-Projekt.
   a. Wurden im Offline-Projekt keine Änderungen vorgenommen, können Sie ohne Hochladen in den Online-Modus schalten. Klicken Sie auf „Go Online“ (Online schalten).
   b. Wurden Änderungen im geöffneten Projekt vorgenommen, die in der Steuerung nicht vorhanden sind, können Sie sich für das Hochladen des Projekts oder das Abbrechen des Hochladens entscheiden oder eine andere Datei auswählen.

   Bei Auswahl von „Upload“ (Hochladen) werden die Standard- und Sicherheitsanwendungen hochgeladen. Ist eine Sicherheits-Task-Signatur vorhanden, wird sie ebenfalls hochgeladen. Der Sicherheitssperrzustand des Projekts zeigt den ursprünglichen Zustand des Online-(Steuerungs-) Projekts an.

HINWEIS Ist vor dem Hochladen eine Offline-Sicherheits-Task-Signatur vorhanden oder ist das Offline-Projekt sicherheitsgesperrt, die Steuerung aber sicherheitsentsperrt oder keine Sicherheits-Task-Signatur vorhanden, werden die Offline-Sicherheits-Task-Signatur und der Sicherheitssperrzustand durch die Online-Werte (sicherheitsentsperrt und ohne Sicherheits-Task-Signatur) ersetzt. Wenn diese Änderungen nicht dauerhaft sein sollen, speichern Sie das Offline-Projekt nach dem Upload-Vorgang nicht ab.

Schalten in den Online-Modus

Gehen Sie wie folgt vor, um in den Online-Modus zu schalten und ein von der Steuerung ausgeführtes Projekt zu überwachen.



1. Legen Sie den Pfad zur Steuerung fest.
   a. Klicken Sie auf „Who Active“ (Aktive Geräte) .
   b. Wählen Sie die Steuerung aus.
   Klicken Sie zum Erweitern einer Ebene auf das Pluszeichen (+). Ist bereits eine Steuerung ausgewählt, stellen Sie sicher, dass es sich um die richtige Steuerung handelt.
2. Klicken Sie auf „Go Online“ (Online schalten).

   Die Anwendung Logix Designer überprüft Folgendes:
   - Stimmen Seriennummern von Offline-Projekt und Steuerung überein, falls die Option „Project to Controller Match “ (Übereinstimmung zwischen Projekt und Steuerung) ausgewählt ist?
   - Enthält das Offline-Projekt Änderungen, die nicht im Steuerungsprojekt enthalten sind?
   - Stimmen die Versionen von Offline-Projekt und Steuerungs-Firmware überein?
   - Sind Offline-Projekt oder Steuerung sicherheitsgesperrt?
   - Besitzen Offline-Projekt oder Steuerung kompatible Sicherheits-Task-Signaturen?
3. Befolgen Sie die Anweisungen in der nachfolgenden Tabelle, um eine Verbindung zur Steuerung herzustellen.

Tabelle 35 – Anschließen an die Steuerung

Zeigt die Software Folgendes an	Dann
Verbindung zur Steuerung nicht möglich. Fehlende Übereinstimmung zwischen der Seriennummer des Offline-Projekts und der Seriennummer der Steuerung. Die ausgewählte Steuerung könnte die falsche Steuerung sein.	Stellen Sie eine Verbindung zur richtigen Steuerung her, wählen Sie eine andere Projektdatei oder das Optionsfeld „Update project serial number“ (Seriennummer des Projekts aktualisieren) und dann „Go Online“ (Online schalten) aus, um eine Verbindung zur Steuerung herzustellen und die Seriennummer des Offline-Projekts entsprechend der Steuerung zu aktualisieren.
Verbindung zur Steuerung nicht möglich. Die Version des Offline-Projekts und die Firmware der Steuerung sind nicht kompatibel.	Wählen Sie eine der folgenden Optionen: • Wählen Sie „Update Firmware“ (Firmware aktualisieren). Klicken Sie nach Auswahl der erforderlichen Version auf „Update“ (Aktualisieren). Klicken Sie auf „Yes“ (Ja), um Ihre Auswahl zu bestätigen. **WICHTIG:** Das Online-Projekt wird gelöscht. • Damit das Online-Projekt erhalten bleibt, brechen Sie den Online-Prozess ab und installieren Sie eine Version der Studio 5000-Umgebung, die mit der Firmware-Version Ihrer Steuerung kompatibel ist.
Sie müssen einen Upload oder Download durchführen, um mit dem geöffneten Projekt in den Online-Modus zu wechseln.	Wählen Sie eine der folgenden Optionen: • „Upload“ (Hochladen), um das Offline-Projekt zu aktualisieren. • „Download“ (Herunterladen), um das Steuerungsprojekt zu aktualisieren. • Wählen Sie „File“ (Datei) aus, um ein anderes Offline-Projekt auszuwählen.
Verbindung unter Erhalt der Sicherheits-Task-Signatur nicht möglich. Die Nebenversion der Steuerungs-Firmware ist mit der Sicherheits-Task-Signatur im Offline-Projekt nicht kompatibel.	• Ist die Nebenversion der Steuerungs-Firmware nicht kompatibel, aktualisieren Sie zur Beibehaltung der Sicherheits-Task-Signatur die Firmware-Version in der Steuerung, sodass sie exakt mit dem Offline-Projekt übereinstimmt. Schalten Sie dann zur Steuerung in den Online-Modus. • Um trotz der Inkompatibilität der Sicherheits-Task-Signatur mit dem Herunterladen fortzufahren, klicken Sie auf „Download“ (Herunterladen). Die Sicherheits-Task-Signatur wird gelöscht. **WICHTIG:** Das Sicherheitssystem erfordert eine erneute Validierung.
Verbindung zur Steuerung nicht möglich. Die inkompatible Sicherheits-Task-Signatur kann nicht gelöscht werden, solange das Projekt sicherheitsgesperrt ist.	Brechen Sie den Online-Prozess ab. Sie müssen das Offline-Projekt zuerst sicherheitsentsperren, bevor Sie versuchen, in den Online-Modus zu schalten.

Wenn die Steuerung und die Anwendung Logix Designer online geschaltet sind, stimmen der Sicherheitssperrzustand und die Sicherheits-Task-Signatur der Steuerung mit dem Projekt der Steuerung überein. Der Sicherheitssperrzustand und die Sicherheits-Task-Signatur des Offline-Projekts werden durch die Steuerung überschrieben. Wenn die Änderungen am Offline-Projekt nicht dauerhaft sein sollen, speichern Sie die Projektdatei nach dem Schalten in den Online-Modus nicht ab.

Speichern und Laden von Projekten mithilfe des nichtflüchtigen Speichers

Thema	Seite
Verwenden von Speicherkarten für nichtflüchtigen Speicher	119
Speichern eines Sicherheitsprojekts	120
Laden eines Sicherheitsprojekts	121
Verwenden von Energiespeichermodulen	122
Abschätzen der ESM-Unterstützung für die Uhrzeit	124
Verwalten der Firmware mit Firmware Supervisor	124

Verwenden von Speicherkarten für nichtflüchtigen Speicher

GuardLogix-Steuerungen der Serie 5570 unterstützen eine Speicherkarte für nichtflüchtigen Speicher. Der nichtflüchtige Speicher ermöglicht das Speichern einer Kopie Ihres Projekts in der Steuerung. Die Steuerung benötigt zum Speichern dieser Kopie keine Stromversorgung oder Batterie.

Sie können das gespeicherte Projekt in folgenden Situationen aus dem nichtflüchtigen Speicher in den Anwenderspeicher der Steuerung laden:

- bei jedem Einschalten
- immer wenn sich kein Projekt in der Steuerung befindet und diese eingeschaltet wird
- jederzeit über die Anwendung Logix Designer

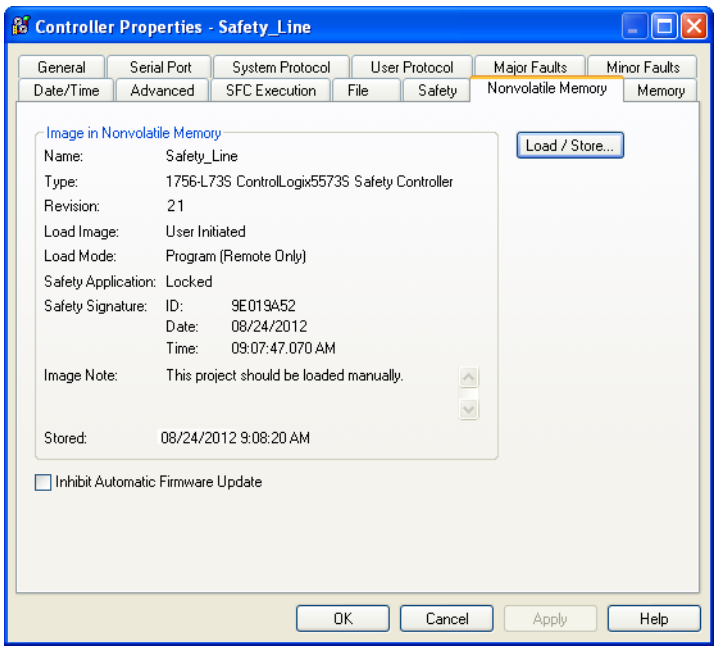
WICHTIG Im nichtflüchtigen Speicher wird der Inhalt des Anwenderspeichers zum Zeitpunkt der Speicherung des Projekts gespeichert:

- Änderungen, die Sie nach dem Speichern des Projekts vornehmen, werden im nichtflüchtigen Speicher nicht nachgeführt.
- Wenn Sie am Projekt vorgenommene Änderungen nicht speichern, werden diese beim Laden des Projekts aus dem nichtflüchtigen Speicher überschrieben. In diesem Fall müssen Sie das Projekt hoch- bzw. herunterladen, um in den Online-Modus schalten zu können.
- Wenn Sie online durchgeführte Änderungen, geänderte Tag-Werte oder einen geänderten ControlNet-Netzwerkplan speichern möchten, müssen Sie das Projekt nach dem Ausführen dieser Änderungen erneut speichern.

ACHTUNG: Entfernen Sie die Speicherkarte nicht, während die Steuerung Daten von der Karte liest oder auf diese schreibt. Dies wird durch ein grünes Blinklicht der Statusanzeige „OK“ signalisiert. Dadurch könnten die Daten auf der Karte oder in der Steuerung beschädigt werden. Auch die zuletzt geladene Firmware in der Steuerung könnte dadurch Schaden nehmen. Lassen Sie die Karte in der Steuerung, bis die Statusanzeige OK kontinuierlich grün leuchtet.

Wenn eine Speicherkarte installiert ist, können Sie den Inhalt der Karte auf der Registerkarte „Nonvolatile Memory“ (Nichtflüchtiger Speicher) im Dialogfenster „Controller Properties“ (Steuerungseigenschaften) anzeigen. Wenn eine Sicherheitsanwendung auf der Karte gespeichert ist, werden der Sicherheitssperrstatus und die Sicherheits-Task-Signatur angezeigt.

Abbildung 30 – Registerkarte „Nonvolatile Memory“ (Nichtflüchtiger Speicher)



Ausführliche Informationen zur Verwendung des nichtflüchtigen Speichers finden Sie in der Publikation 1756-PM017, Logix5000 Controllers Nonvolatile Memory Programming Manual.

Speichern eines Sicherheitsprojekts

Sie können ein Sicherheitsprojekt nicht speichern, wenn der Status der Sicherheits-Task „Safety Task Inoperable“ (Sicherheits-Task nicht funktionsbereit) lautet. Wenn Sie ein Sicherheitsprojekt speichern, wird die Firmware der Primärsteuerung und des Sicherheitspartners auf der Speicherkarte gespeichert.

Wenn die Steuerung kein Anwendungsprojekt enthält, können Sie die Firmware der Sicherheitssteuerung nur speichern, wenn eine gültige Partnerschaft vorhanden ist. Durch das alleinige Laden der Firmware wird die Bedingung „Safety Task Inoperable“ (Sicherheits-Task nicht funktionsbereit) nicht gelöscht.

Wenn beim Speichern eines Projekts eine Sicherheits-Task-Signatur vorhanden ist:

- werden Sicherheits-Tags mit dem Wert gespeichert, den sie beim ersten Erstellen der Signatur aufwiesen.
- werden Standard-Tags aktualisiert.
- wird die aktuelle Sicherheits-Task-Signatur gespeichert.

Wenn Sie ein Sicherheitsanwendungsprojekt auf eine Speicherkarte speichern, sollten Sie als Lademodus die Option „Program (Remote Only)“ (Programm (nur dezentral)) auswählen, also den Modus, in den die Steuerung nach dem Laden wechseln soll.

Laden eines Sicherheitsprojekts

Sie können einen Ladevorgang vom nichtflüchtigen Speicher nur unter folgenden Bedingungen einleiten:

- Der Steuerungstyp, der von dem im nichtflüchtigen Speicher abgelegten Projekt angegeben wird, stimmt mit dem Steuerungstyp überein.
- Die Haupt- und Nebenversionen des Projekts im nichtflüchtigen Speicher stimmen mit den Haupt- und Nebenversionen auf der Steuerung überein.
- Ihre Steuerung befindet sich nicht im Run-Modus.

Es gibt mehrere Möglichkeiten, wann (unter welchen Bedingungen) ein Projekt in den Anwenderspeicher der Steuerung geladen werden kann.

Tabelle 36 – Optionen zum Laden eines Projekts

Laden des Projekts	Auswahl dieser „Load Image“-Option (Abbilddatei laden)	Hinweise
Bei jedem Einschalten oder Aus- und Wiedereinschalten	On Power Up (Beim Einschalten)	• Beim Aus- und Einschalten der Versorgungsspannung gehen alle online durchgeführten Änderungen, geänderten Tag-Werte und Netzwerkpläne verloren, sofern Sie diese nicht in den nichtflüchtigen Speicher geschrieben haben. • Die Steuerung lädt das gespeicherte Projekt und die Firmware bei jedem Einschalten (unabhängig von der Firmware oder dem Anwendungsprojekt in der Steuerung). Der Ladevorgang findet statt, ganz gleich, ob die Steuerung sicherheitsgesperrt ist oder über eine Sicherheits-Task-Signatur verfügt. • Sie können immer die Anwendung Logix Designer zum Laden des Projekts verwenden.
Wenn sich kein Projekt in der Steuerung befindet und Sie die Spannungsversorgung des Chassis einschalten oder aus- und wieder einschalten	On Corrupt Memory (Bei beschädigtem Speicher)	• Wenn beispielsweise die Batterie entladen ist und die Spannungsversorgung der Steuerung unterbrochen ist, wird das Projekt aus dem Speicher gelöscht. Beim Wiederherstellen der Spannungsversorgung wird bei dieser Ladeoption das Projekt wieder in die Steuerung geladen. • Die Steuerung aktualisiert die Firmware in der Primärsteuerung oder im Sicherheitspartner, sofern erforderlich. Das im nichtflüchtigen Speicher abgelegte Anwendungsprojekt wird ebenfalls geladen, während die Steuerung in den ausgewählten Modus (Program oder Run) wechselt. • Sie können immer die Anwendung Logix Designer zum Laden des Projekts verwenden.
Nur über die Anwendung Logix Designer	User Initiated (Vom Anwender initiiert)	• Wenn der Steuerungstyp und die Haupt- und Nebenversionen des Projekts im nichtflüchtigen Speicher mit dem Steuerungstyp und den Haupt- sowie Nebenversionen der Steuerung übereinstimmen, können Sie einen Ladevorgang einleiten (unabhängig vom Status der Sicherheits-Task). • Ein Projekt kann nur auf eine sicherheitsgesperrte Steuerung geladen werden, wenn die im nichtflüchtigen Speicher des Projekts abgelegte Sicherheits-Task-Signatur mit der Signatur des Projekts in der Steuerung übereinstimmt. • Stimmen die Signaturen nicht überein bzw. ist die Steuerung ohne Sicherheits-Task-Signatur sicherheitsgesperrt, werden Sie aufgefordert, zunächst die Steuerung zu entsperren. **WICHTIG:** Wenn Sie die Steuerung entsperren und einen Ladevorgang aus dem nichtflüchtigen Speicher einleiten, werden nach Abschluss des Ladevorgangs Sicherheitssperrstatus, Kennwörter und Sicherheits-Task-Signatur auf die Werte im nichtflüchtigen Speicher gesetzt. • Stimmt die Firmware der Primärsteuerung mit der Version im nichtflüchtigen Speicher überein, wird die Firmware des Sicherheitspartners aktualisiert, sofern erforderlich; die im nichtflüchtigen Speicher abgelegte Anwendung wird geladen, sodass der Sicherheits-Task-Status „Safety Task Operable“ (Sicherheits-Task funktionsbereit) lautet und die Steuerung in den ausgewählten Modus (Program oder Run) wechselt.

WICHTIG Vergewissern Sie sich vor der Verwendung der Software ControlFLASH, dass die SD-Karte entsperrt ist, wenn „On Power Up“ (Beim Einschalten) ausgewählt ist. Andernfalls werden die aktualisierten Daten möglicherweise von der Firmware auf der Speicherkarte überschrieben.

Verwenden von Energiespeichermodulen

Sie können die GuardLogix-Energiespeichermodule (ESMs) zur Ausführung der folgenden Aufgaben verwenden:

- Versorgen der Steuerung mit Spannung, um das Programm im integrierten, nichtflüchtigen Speicher der Steuerung speichern zu können, nachdem die Spannungsversorgung zum Chassis unterbrochen wurde oder nachdem die Steuerung aus einem eingeschalteten Chassis ausgebaut wurde.

  WICHTIG Wenn Sie ein ESM zum Speichern des Programms im integrierten, nichtflüchtigen Speicher verwenden, speichern Sie das Programm **nicht** auf der in der Steuerung installierten SD-Karte.

- Löschen des Programms aus dem integrierten, nichtflüchtigen Speicher der Steuerung. Weitere Informationen finden Sie unter Löschen des Programms aus dem integrierten nichtflüchtigen Speicher.

In der folgenden Tabelle sind die ESMs beschrieben.

Tabelle 37 – Energiespeichermodule

Best.- Nr.	Beschreibung
1756-ESMCAP(XT)	Kondensatorbasiertes ESM In den Steuerungen ist dieses ESM bereits vorinstalliert.
1756-ESMNSE(XT)	Kondensatorbasiertes ESM ohne Backupleistung für die Uhrzeit Verwenden Sie dieses ESM, wenn für Ihre Anwendung das installierte ESM seine gespeicherte Restenergie auf 40 µJ oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder aus ihr ausgebaut werden kann. Außerdem können Sie dieses ESM nur mit der Steuerung 1756-L73S (8 MB) oder einer Steuerung mit kleinerem Speicher verwenden.
1756-ESMNRM(XT)	Sicheres kondensatorbasiertes ESM (kann nicht ausgebaut werden) Dieses ESM bietet Ihrer Anwendung verbesserte Sicherheit, da es den physischen Zugriff auf den USB-Anschluss und die SD-Karte verhindert.
1756-SPESMNSE(XT)	Kondensatorbasiertes ESM ohne Uhrzeit-Backupleistung für den Sicherheitspartner Verwenden Sie dieses ESM, wenn für Ihre Anwendung das installierte ESM seine gespeicherte Restenergie auf 40 µJ oder weniger abbauen muss, bevor es in Ihre Anwendung integriert oder daraus ausgebaut werden kann. Im Sicherheitspartner für den Einsatz unter extremen Umgebungsbedingungen 1756-L7SPXT ist das 1756-SPESMNSEXT vorinstalliert.
1756-SPESMNRM(XT)	Sicheres kondensatorbasiertes ESM (kann nicht ausgebaut werden) für den Sicherheitspartner

Speichern des Programms im integrierten, nichtflüchtigen Speicher

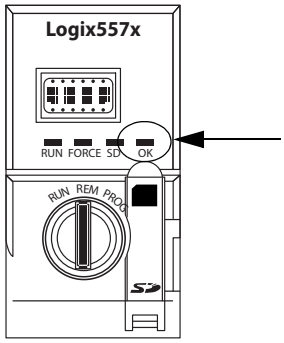
Gehen Sie wie folgt vor, um das Programm im nichtflüchtigen Speicher zu speichern, wenn die Spannungsversorgung der Steuerung unterbrochen wird.

1. Unterbrechen Sie die Spannungsversorgung der Steuerung.

   Dazu haben Sie zwei Möglichkeiten:
   - Ausschalten der Chassisspannung, während die Steuerung im Chassis installiert ist.
   - Ausbauen der Steuerung aus einem eingeschalteten Chassis.

Sobald die Steuerung nicht mehr mit Spannung versorgt wird, leuchtet die Statusleuchte „OK“ bis nach Abschluss der Programmspeicherung rot.

Abbildung 31 – Statusleuchte „OK“.



2. Lassen Sie das ESM in der Steuerung, bis die Statusleuchte „OK“ erlischt.

3. Bauen Sie, wenn erforderlich, das ESM aus der Steuerung aus, wenn die rote Statusleuchte „OK“ erloschen ist.

Löschen des Programms aus dem integrierten nichtflüchtigen Speicher

Gehen Sie, wenn Ihre Anwendung es zulässt, wie folgt vor, um das Programm aus dem integrierten, nichtflüchtigen Speicher der Steuerung zu löschen.

1. Bauen Sie das ESM aus der Steuerung aus.

2. Unterbrechen Sie die Spannungsversorgung der Steuerung, indem Sie die Chassisspannung, während die Steuerung im Chassis installiert ist, ausschalten oder die Steuerung aus einem eingeschalteten Chassis ausbauen.

3. Bauen Sie das ESM wieder in die Steuerung ein.

4. Stellen Sie die Spannungsversorgung der Steuerung wieder her.
   a. Wenn die Steuerung bereits im Chassis installiert ist, schalten Sie die Spannungsversorgung des Chassis wieder ein.
   b. Wenn die Steuerung nicht im Chassis installiert ist, installieren Sie zunächst die Steuerung wieder im Chassis und schalten Sie dann das Chassis wieder ein.

Abschätzen der ESM-Unterstützung für die Uhrzeit

Das ESM unterstützt die Aufrechterhaltung der Uhrzeit der Steuerung (Attribut „WallClockTime“), wenn die Spannungsversorgung unterbrochen wurde. Verwenden Sie die folgende Tabelle, um die die Haltezeit des ESM auf der Grundlage der Temperatur der Steuerung und des installierten ESM abzuschätzen.

Tabelle 38 – Temperatur ggü. Haltezeit

Temperatur	Haltezeit (in Tagen)		
	1756-ESMCAP(XT)	1756-ESMNRM(XT) 1756-SPESMNRM(XT)	1756-ESMNSE(XT) 1756-SPESMNSE(XT)
20 °C	12	12	0
40 °C	10	10	0
60 °C	7	7	0

Verwalten der Firmware mit Firmware Supervisor

Sie können die Funktion „Firmware Supervisor“ zum Verwalten der Firmware auf Steuerungen verwenden. Firmware Supervisor ermöglicht Steuerungen die automatische Aktualisierung von Geräten:

- Lokale und dezentrale Module können aktualisiert werden, wenn sie sich im Programm- oder Run-Modus befinden.
- Für eine exakte Übereinstimmung muss die elektronische Codierung konfiguriert werden.
- Das Firmware-Kit für das Zielgerät muss sich auf der Speicherkarte der Steuerung befinden.
- Das Gerät muss Firmware-Upgrades über die Software ControlFLASH unterstützen.

Nicht modulare, dezentrale E/A-Produkte, die sich direkt auf dem Netzwerk befinden, werden auch ohne Adapter von der Funktion Firmware Supervisor unterstützt. Hierzu zählen Sicherheits-E/A-Geräte in EtherNet/IP-Netzwerken. Sicherheits-E/A-Geräte in DeviceNet-Netzwerken und POINT Guard-E/A-Module werden noch nicht unterstützt.

Gehen Sie wie folgt vor, um Firmware Supervisor zu aktivieren.

1. Klicken Sie im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) auf die Registerkarte „Nonvolatile Memory“ (Nichtflüchtiger Speicher).
2. Klicken Sie auf „Load/Store“ (Laden/Speichern).
3. Wählen Sie im Pulldown-Menü „Automatic Firmware Updates“ (Automatische Firmware-Updates) die Optionen „Enable“ (Aktivieren) und „Store Files to Image“ (Dateien in Abbilddatei speichern) aus.

Die Anwendung Logix Designer verschiebt die Firmware-Kits von Ihrem Computer auf die Speicherkarte der Steuerung, damit sie von Firmware Supervisor verwendet werden können.

HINWEIS Wenn Sie die Funktion Firmware Supervisor deaktivieren, deaktivieren Sie nur die über Firmware Supervisor vorgenommenen Updates. Hierzu zählen jedoch nicht die Firmware-Updates der Steuerung, die vorgenommen werden, wenn das Steuerungsabbild erneut von der Speicherkarte geladen wird.

Zustandsüberwachung und Fehlerbehebung

Thema	Seite
Anzeige des Status über die Online-Leiste	125
Überwachen der Verbindungen	126
Überwachen von Status-Flags	127
Überwachen des Sicherheitsstatus	128
Steuerungsfehler	128
Entwickeln einer Fehlerroutine	131

Informationen zur Interpretation der Statusleuchten und Fehlermeldungen der Steuerung finden Sie in Anhang A, Statusanzeigen.

Anzeige des Status über die Online-Leiste

Die Online-Leiste zeigt Projekt- und Steuerungsinformationen an, einschließlich Steuerungsstatus, Force-Zustand, Online-Bearbeitungsstatus und Sicherheitsstatus.

Abbildung 32 – Statusschaltflächen

Wenn die Schaltfläche „Controller Status“ (Steuerungsstatus), wie vorstehend abgebildet, ausgewählt ist, zeigt die Online-Leiste den Steuerungsmodus (RUN) und den Status (OK) an. Die Anzeige BAT kombiniert den Status von Primärsteuerung und Sicherheitspartner. Falls einer oder beide einen Batteriefehler aufweist/aufweisen, leuchtet die Statusanzeige auf. Die Anzeige I/O kombiniert den Status von Standard- und Sicherheits-E/A und verhält sich genau wie die Statusanzeige auf der Steuerung. Das E/A-Modul mit dem schwerwiegendsten Fehlerzustand wird neben der Statusanzeige eingeblendet.

Wenn die Schaltfläche „Safety Status“ (Sicherheitsstatus) ausgewählt ist, wie nachfolgend dargestellt, zeigt die Online-Leiste die Sicherheits-Task-Signatur an.

Abbildung 33 – Online-Anzeige der Sicherheitssignatur

Die Schaltfläche „Safety Status“ (Sicherheitsstatus) selbst zeigt an, ob die Steuerung sicherheitsgesperrt bzw. -entsperrt oder fehlerhaft ist. Sie zeigt auch ein Symbol an, das den Sicherheitsstatus beschreibt.

Tabelle 39 – Sicherheitsstatussymbol

Sicherheitsstatus:	Angezeigtes Symbol:
Sicherheits-Task OK	
Sicherheits-Task nicht funktionsbereit	
Partner fehlt Partner nicht verfügbar Hardware inkompatibel Firmware inkompatibel	
Offline	

Die Symbole sind grün, wenn die Steuerung sicherheitsgesperrt ist, gelb, wenn die Steuerung sicherheitsentsperrt ist und rot, wenn bei der Steuerung ein Sicherheitsfehler vorliegt. Wenn eine Sicherheits-Task-Signatur vorliegt, ist das Symbol mit einem kleinen Kontrollhäkchen versehen.

Überwachen der Verbindungen

Sie können den Status von Standard- und Sicherheitsverbindungen überwachen.

Alle Verbindungen

Falls 100 ms lang keine Kommunikation mit einem Gerät in der E/A-Konfiguration der Steuerung stattfindet, erfolgt ein Kommunikations-Timeout und die Steuerung gibt folgende Warnmeldungen aus:

- Die Anzeige „I/O“ (E/A) auf der Vorderseite der Steuerung blinkt grün.
- Ein Warnsymbol ⚠ wird über dem E/A-Konfigurationsordner und über dem Gerät, bei dem ein Timeout aktiviert wurde, angezeigt.
- Ein Gerätefehler wird erzeugt, auf den Sie über die Registerkarte „Connection“ (Verbindung) im Dialogfeld „Module Properties“ (Moduleigenschaften) für das Gerät oder über den GSV-Befehl zugreifen können.

ACHTUNG: Sicherheits-E/A und Producer-/Consumer-Verbindungen können nicht so konfiguriert werden, dass die Steuerung bei einem Verbindungsausfall automatisch in den Fehlerzustand übergeht. Daher müssen Sie die Verbindungsfehler überwachen, um sicherzustellen, dass das Sicherheitssystem die SIL 3/PLe-Integrität beibehält.

Siehe Sicherheitsverbindungen auf Seite 127.

Sicherheitsverbindungen

Für Tags, die zu produzierten oder konsumierten Sicherheitsdaten gehören, können Sie den Status der Sicherheitsverbindungen mithilfe des Glieds CONNECTION_STATUS überwachen. Für die Überwachung von Eingangs- und Ausgangsverbindungen haben Sicherheits-E/A-Tags ein Verbindungsstatusglied mit dem Namen SafetyStatus. Beide Datentypen enthalten zwei Bits: RunMode und ConnectionFaulted.

Der RunMode-Wert zeigt an, ob konsumierte Daten gerade aktiv durch ein Gerät aktualisiert werden, das sich im Run-Modus (1) oder im Leerlaufstatus (0) befindet. Der Leerlaufstatus wird angezeigt, wenn die Verbindung geschlossen ist, die Sicherheits-Task fehlerhaft ist oder sich die dezentrale Steuerung oder das dezentrale Gerät im Programm- oder Testmodus befindet.

Der ConnectionFaulted-Wert zeigt an, ob die Sicherheitsverbindung zwischen dem Sicherheits-Producer und dem Sicherheits-Consumer gültig (Valid) (0) oder fehlerhaft (Faulted) (1) ist. Falls ConnectionFaulted infolge eines Verlusts der physischen Verbindung auf fehlerhaft (1) gesetzt wird, werden die Sicherheitsdaten auf null zurückgesetzt.

Die nachfolgende Tabelle beschreibt die Kombinationen der RunMode- und ConnectionFaulted-Zustände.

Tabelle 40 – Sicherheitsverbindungsstatus

RunMode-Status	ConnectionFaulted-Status	Betrieb der Sicherheitsverbindung
1 = Run	0 = gültig	Die Daten werden aktiv vom produzierenden Gerät gesteuert. Das produzierende Gerät befindet sich im Run-Modus.
0 = Leerlauf	0 = gültig	Die Verbindung ist aktiv und das produzierende Gerät befindet sich im Leerlauf. Die Sicherheitsdaten werden auf null zurückgesetzt.
0 = Leerlauf	1 = fehlerhaft	Die Sicherheitsverbindung ist fehlerhaft. Der Status des produzierenden Geräts ist unbekannt. Die Sicherheitsdaten werden auf null zurückgesetzt.
1 = Run	1 = fehlerhaft	Ungültiger Status.

Falls ein Gerät gesperrt ist, wird das ConnectionFaulted-Bit auf fehlerhaft (1) und das RunMode-Bit auf Leerlauf (0) gesetzt, und zwar für jede Verbindung, die mit dem Gerät besteht. Als Folge werden die konsumierten Sicherheitsdaten auf null zurückgesetzt.

Überwachen von Status-Flags

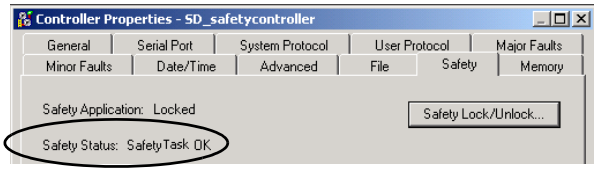
Logix-Steuerungen, einschließlich GuardLogix-Steuerungen, unterstützen Statuskennwörter, die Sie in Ihrer Logik zur Überwachung bestimmter Ereignisse verwenden können.

Weitere Informationen zur Verwendung dieser Kennwörter finden Sie in der Publikation 1756-PM015, Logix5000 Controllers Controller Information and Status Programming Manual.

Überwachen des Sicherheitsstatus

Sie können Informationen zum Sicherheitsstatus der Steuerung in der Online-Leiste über die Schaltfläche zum Sicherheitsstatus und auf der Registerkarte „Safety“ (Sicherheit) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften) aufrufen.

Abbildung 34 – Status der Sicherheits-Task



Die möglichen Werte für den Sicherheitsstatus sind:

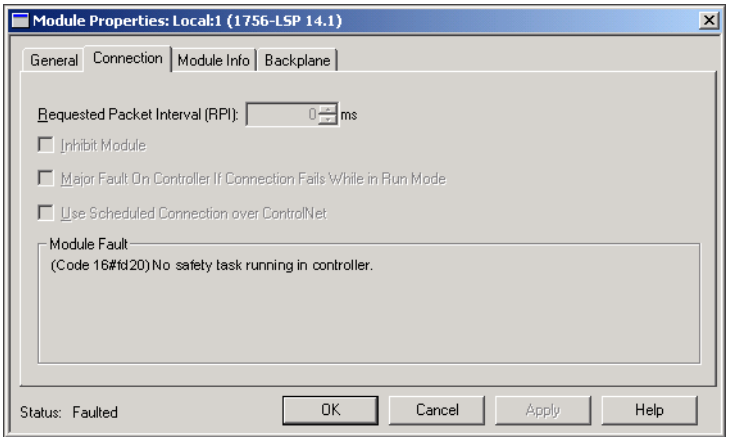
- Sicherheitspartner fehlt oder ist nicht verfügbar.
- Sicherheitspartner-Hardware ist nicht kompatibel mit der Primärsteuerung.
- Sicherheitspartner-Firmware ist nicht kompatibel mit der Primärsteuerung.
- Sicherheits-Task nicht funktionsbereit.
- Sicherheits-Task OK.

Mit Ausnahme von „Sicherheits-Task OK“ zeigen die oben genannten Beschreibungen, dass ein nicht korrigierbarer Sicherheitsfehler vorliegt.

Die Fehlercodes und erforderlichen Maßnahmen finden Sie im Abschnitt Schwerwiegende Sicherheitsfehler (Typ 14) auf Seite 130.

Der Status des Sicherheitspartners kann auf der Registerkarte „Connection“ (Verbindung) des Dialogfelds „Module Properties“ (Moduleigenschaften) eingesehen werden.

Abbildung 35 – Status des Sicherheitspartners



Steuerungsfehler

Bei Fehlern im GuardLogix-System kann es sich um nicht korrigierbare Steuerungsfehler, nicht korrigierbare Sicherheitsfehler in der Sicherheitsanwendung oder korrigierbare Sicherheitsfehler in der Sicherheitsanwendung handeln.

Nicht korrigierbare Steuerungsfehler

Diese treten auf, wenn die interne Diagnose der Steuerung fehlschlägt. Wenn ein nicht korrigierbarer Steuerungsfehler auftritt, stoppt die Ausführung der Sicherheits-Task und die Sicherheits-E/A-Geräte werden in den sicheren Zustand versetzt. Die Wiederherstellung des korrekten Betriebs erfordert ein erneutes Herunterladen des Anwendungsprogramms.

Nicht korrigierbare Sicherheitsfehler in der Sicherheitsanwendung

Wenn ein nicht korrigierbarer Sicherheitsfehler in der Sicherheitsanwendung auftritt, werden die Sicherheitslogik und das Sicherheitsprotokoll beendet. Fehler beim Sicherheits-Task-Watchdog und bei der Steuerungspartnerschaft fallen in diese Kategorie.

Falls die Sicherheits-Task einen nicht korrigierbaren Sicherheitsfehler erkennt, der im Fehlerbehebungsprogramm der Steuerung gelöscht wird, wird die Standardanwendung weiter ausgeführt.

ACHTUNG: Ein Sicherheitsfehler wird durch Überschreiben nicht gelöscht. Wenn Sie den Sicherheitsfehler überschreiben, obliegt es Ihnen, zu beweisen, dass durch diese Maßnahme der sichere Betrieb nicht beeinträchtigt wird.

Sie müssen Ihrer Zertifizierungsstelle den Beweis erbringen, dass durch das Überschreiben des Sicherheitsfehlers der sichere Betrieb aufrecht erhalten bleibt.

Falls eine Sicherheits-Task-Signatur vorliegt, können Sie den Fehler löschen, damit die Sicherheits-Task arbeiten kann. Falls keine Sicherheits-Task-Signatur vorliegt, funktioniert die Sicherheits-Task erst wieder, nachdem die gesamte Anwendung erneut heruntergeladen wurde.

Korrigierbare Sicherheitsfehler in der Sicherheitsanwendung

Wenn ein korrigierbarer Fehler in der Sicherheitsanwendung auftritt, kann das System die Ausführung der Sicherheits-Task abhängig davon anhalten, ob der Fehler durch das Fehlerbehebungsprogramm in der Sicherheitsanwendung bearbeitet wird oder nicht.

Falls ein korrigierbarer Fehler durch das Programm gelöscht wird, fährt die Sicherheits-Task ohne Unterbrechung mit der Ausführung fort.

Falls ein korrigierbarer Fehler in der Sicherheitsanwendung nicht durch das Programm gelöscht wird, tritt ein korrigierbarer Fehler vom Typ 14, Code 2, auf. Die Ausführung des Sicherheitsprogramms wird gestoppt und die Sicherheitsprotokollverbindungen werden geschlossen und zur Reinitialisierung neu geöffnet. Sicherheitsausgänge werden in den sicheren Zustand geschaltet und der Producer der konsumierten Sicherheits-Tags erteilt den Consumern den Befehl, sie ebenfalls in einen sicheren Zustand zu schalten.

Korrigierbare Fehler ermöglichen es Ihnen, die Standard- und/oder Sicherheitsanwendung sowie die Ursache des Fehlers entsprechend zu korrigieren. Falls jedoch eine Sicherheits-Task-Signatur vorliegt oder die Steuerung sicherheitsgesperrt ist, müssen Sie zuerst die Steuerung entsperren und die Sicherheits-Task-Signatur löschen, bevor Sie die Sicherheitsanwendung bearbeiten können.

Anzeigen von Fehlern

Das Dialogfeld „Recent Faults“ (Letzte Fehler) auf der Registerkarte „Major Faults“ (Schwerwiegende Fehler) des Dialogfelds „Controller Properties“ (Steuerungseigenschaften) enthält zwei Unter-Registerkarten: eine für Standardfehler und eine für Sicherheitsfehler.

Die Statusanzeige auf der Steuerung gibt auch Fehlercodes zusammen mit einer kurzen Beschreibung an (siehe ab Seite 133).

Fehlercodes

Tabelle 41 enthält die Fehlercodes, die sich speziell auf GuardLogix-Steuerungen beziehen. Typ und Code entsprechen dem Typ und dem Code auf der Registerkarte „Major Faults“ (Schwerwiegende Fehler) im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) und im Objekt PROGRAM, Attribut MAJORFAULTRECORD bzw. MINORFAULTRECORD.

Tabelle 41 – Schwerwiegende Sicherheitsfehler (Typ 14)

Code	Ursache	Status	Erforderliche Maßnahmen
01	Task-Watchdog abgelaufen. Anwender-Task konnte nicht in einem spezifizierten Zeitraum abgeschlossen werden. Ein Programmfehler hat eine Endlosschleife verursacht, das Programm ist zu komplex, um so schnell wie angegeben zu arbeiten, eine Task höherer Priorität verhindert die Beendigung dieser Task oder der Sicherheitspartner wurde entfernt.	Nicht korrigierbar	Den Fehler löschen. Falls eine Sicherheits-Task-Signatur vorliegt, wird der Sicherheitsspeicher neu initialisiert und die Sicherheits-Task beginnt mit der Ausführung. Falls keine Sicherheits-Task-Signatur vorliegt, müssen Sie das Programm erneut herunterladen, damit die Sicherheits-Task ausgeführt werden kann. Setzen Sie den Sicherheitspartner wieder ein, falls er entfernt wurde.
02	Ein Fehler liegt in einer Routine der Sicherheits-Task vor.	korrigierbar	Korrigieren Sie den Fehler in der Anwenderprogrammlogik.
03	Sicherheitspartner fehlt.	Nicht korrigierbar	Installieren Sie einen kompatiblen Sicherheitspartner.
04	Sicherheitspartner ist nicht verfügbar.	Nicht korrigierbar	Installieren Sie einen kompatiblen Sicherheitspartner.
05	Sicherheitspartner-Hardware ist nicht kompatibel.	Nicht korrigierbar	Installieren Sie einen kompatiblen Sicherheitspartner.
06	Sicherheitspartner-Firmware ist nicht kompatibel.	Nicht korrigierbar	Aktualisieren Sie den Sicherheitspartner, sodass die Haupt- und Nebenversion der Firmware mit der Primärsteuerung übereinstimmen.
07	Sicherheits-Task ist nicht funktionsbereit. Dieser Fehler tritt auf, wenn die Sicherheitslogik ungültig ist, also wenn z. B. eine nicht übereinstimmende Logik zwischen der Primärsteuerung und dem Sicherheitspartner vorliegt, ein Timeout des Überwachungszeitraums aktiviert wurde oder wenn der Speicher fehlerhaft ist.	Nicht korrigierbar	Den Fehler löschen. Falls eine Sicherheits-Task-Signatur vorhanden ist, wird der Sicherheitsspeicher über die Sicherheits-Task-Signatur erneut initialisiert und die Sicherheits-Task beginnt mit der Ausführung. Falls keine Sicherheits-Task-Signatur vorliegt, müssen Sie das Programm erneut herunterladen, damit die Sicherheits-Task ausgeführt werden kann.
08	Koordinierte Systemzeit (CST) nicht gefunden.	Nicht korrigierbar	Den Fehler löschen. Konfigurieren Sie ein Gerät als CST-Master.
09	Nicht korrigierbarer Steuerungsfehler des Sicherheitspartners.	Nicht korrigierbar	Löschen Sie den Fehler und laden Sie das Programm erneut herunter. Falls das Problem weiterhin besteht, ersetzen Sie den Sicherheitspartner.

Die Publikation 1756-PM014, Logix5000 Controllers Major and Minor Faults Programming Manual, enthält Beschreibungen der Fehlercodes, die häufig für Logix-Steuerungen angezeigt werden.

Entwickeln einer Fehlerroutine

Wenn ein Fehlerzustand auftritt, der so schwerwiegend ist, dass die Steuerung abschaltet, generiert die Steuerung einen schwerwiegenden Fehler und stoppt die Ausführung der Logik.

Abhängig von der jeweiligen Anwendung kann es unter Umständen nicht erwünscht sein, dass alle Sicherheitsfehler das gesamte System abschalten. In solchen Situationen kann eine Fehlerroutine eingesetzt werden, durch die ein spezifischer Fehler gelöscht und damit die Fortsetzung des Betriebs des Standardsteuerungsteils des Systems ermöglicht wird, oder einige Ausgänge können so konfiguriert werden, dass sie eingeschaltet bleiben.

ACHTUNG: Sie müssen Ihrer Zertifizierungsstelle den Beweis erbringen, dass durch das Überschreiben des Sicherheitsfehlers der sichere Betrieb aufrecht erhalten bleibt.

Die Steuerung unterstützt zwei Ebenen zur Handhabung schwerwiegender Fehler:

- Programmfehlerroutine
- Steuerungsfehlerbehebungsprogramm

Beide Routineprogramme können die GSV- und SSV-Befehle, wie auf Seite 132 beschrieben, verwenden.

Programmfehlerroutine

Für jedes Programm kann eine eigene Fehlerroutine verwendet werden. Die Steuerung führt die Programmfehlerroutine aus, wenn ein Befehl fehlerhaft ausgeführt wird. Löscht die Programmfehlerroutine den Fehler nicht oder ist keine Programmfehlerroutine vorhanden, beginnt die Steuerung mit der Ausführung des Steuerungsfehlerbehebungsprogramms, sofern vorhanden.

Steuerungsfehlerbehebungsprogramm

Das Steuerungsfehlerbehebungsprogramm ist eine optionale Komponente, die ausgeführt wird, wenn die Programmfehlerroutine den Fehler nicht löschen kann oder eine solche nicht existiert.

Sie können ein (1) Programm zur Behebung von Steuerungsfehlern erstellen. Nachdem Sie das Programm erstellt haben, müssen Sie eine Routine als Hauptroutine konfigurieren.

Die Publikation 1756-PM014, Logix5000 Controllers Major and Minor Faults Programming Manual, enthält Informationen zum Erstellen und Testen einer Fehlerroutine.

Verwendung der GSV/SSV-Befehle

Logix-Steuerungen speichern Systemdaten in Objekten und nicht in Statusdateien. Sie können die Befehle „Systemwert abrufen“ (GSV) und „Systemwert einstellen“ (SSV) verwenden, um die Steuerungsdaten zu erhalten und einzustellen.

Der GSV-Befehl ruft die spezifizierten Informationen ab und setzt sie an das spezifizierte Ziel. Der SSV-Befehl ändert das spezifizierte Attribut mit Daten von der Quelle des Befehls. Wenn Sie einen GSV- oder SSV-Befehl eingeben, zeigt die Programmiersoftware die Objektklassen, Objektnamen und Attributnamen für jeden Befehl an.

Für Standard-Tasks können Sie den GSV-Befehl verwenden, um die Werte für die verfügbaren Attribute zu erhalten. Bei Verwendung des SSV-Befehls zeigt die Software nur die Attribute an, die Sie festlegen können.

Für die Sicherheits-Task sind die GSV- und SSV-Befehle restriktiver. Die SSV-Befehle in Sicherheits- und Standard-Tasks können das Bit 0 (schwerwiegender Fehler) im Modusattribut eines Sicherheits-E/A-Geräts nicht setzen.

Für Sicherheitsobjekte zeigt Tabelle 42, für welche Attribute Sie mit dem GSV-Befehl Werte abrufen können und welche Attribute Sie mit dem SSV-Befehl in Sicherheits- und Standard-Tasks festlegen können.

ACHTUNG: Gehen Sie vorsichtig bei der Verwendung der GSV-/SSV-Befehle vor. Änderungen an Objekten können zu unvorhergesehenem Steuerungsbetrieb oder Verletzungen des Bedienerpersonals führen.

Tabelle 42 – GSV/SSV-Zugänglichkeit

Sicherheitsobjekt	Attributname	Datentyp	Attributbeschreibung	Zugänglich über Sicherheits-Task		Zugänglich über Standard-Task	
				GSV	SSV	GSV[4]	SSV
Sicherheits-Task	Instance	DINT	Liefert die Instanznummer dieses Task-Objekts. Gültige Werte sind 0 bis 31.	x		x	
	MaximumInterval	DINT[2]	Das maximale Zeitintervall zwischen aufeinanderfolgenden Ausführungen dieser Task.			x	x
	MaximumScanTime	DINT	Aufgezeichnete maximale Ausführungszeit (ms) für diese Task.			x	x
	MinimumInterval	DINT[2]	Das minimale Zeitintervall zwischen aufeinanderfolgenden Ausführungen dieser Task.			x	x
	Priority	INT	Relative Priorität dieser Task im Vergleich zu anderen Tasks. Gültige Werte sind 0 bis 15.	x		x	
	Rate	DINT	Zeitspanne für die Task (in ms), oder Timeout-Wert für die Task (in ms).	x		x	
	Watchdog	DINT	Zeitlimit (in ms) für die Ausführung aller Programme, die mit dieser Task assoziiert sind.	x		x	
Sicherheitsprogramm	Instance	DINT	Liefert die Instanznummer dieses Programmobjekts.	x		x	
	MajorFaultRecord[1]	DINT[11]	Zeichnet schwerwiegende Fehler für dieses Programm auf.	x	x	x	
	MaximumScanTime	DINT	Aufgezeichnete maximale Ausführungszeit (ms) für dieses Programm.			x	x
Sicherheitsroutine	Instance	DINT	Liefert die Instanznummer dieses Routineobjekts. Gültige Werte sind 0 bis 65.535.	x			

Tabelle 42 – GSV/SSV-Zugänglichkeit (Fortsetzung)

Sicherheitsobjekt	Attributname	Datentyp	Attributbeschreibung	Zugänglich über Sicherheits-Task		Zugänglich über Standard-Task	
				GSV	SSV	GSV[4]	SSV
Sicherheitssteuerung	SafetyLocked	SINT	Zeigt, ob die Steuerung sicherheitsgesperrt oder sicherheitsentsperrt ist.	x		x	
	SafetyStatus[2]	INT	Legt den Sicherheitsstatus wie folgt fest als: • Sicherheits-Task OK. (1000000000000000) • Sicherheits-Task nicht funktionsbereit. (1000000000000001) • Partner fehlt. (0000000000000000) • Partner nicht verfügbar. (0000000000000001) • Hardware inkompatibel. (0000000000000010) • Firmware inkompatibel. (0000000000000011)			x	
	SafetySignatureExists	SINT	Zeigt an, ob eine Sicherheits-Task-Signatur vorliegt.	x		x	
	SafetySignatureID	DINT	32-Bit-Identifikationsnummer.			x	
	SafetySignature	String[3]	32-Bit-Identifikationsnummer.			x	
	SafetyTaskFaultRecord[1][2]	DINT[11]	Zeichnet Sicherheits-Task-Fehler auf.			x	
AOI (Sicherheit)	LastEditDate	LINT	Datum- und Uhrzeitstempel der letzten Änderung an der Definition eines Add-On-Befehls.			x	
	SignatureID	DINT	ID-Nummer.			x	
	SafetySignatureID	DINT	32-Bit-Identifikationsnummer.			x	

(1) Weitere Informationen dazu, wie Sie auf dieses Attribut zugreifen können, finden Sie im Abschnitt Zugreifen auf die „FaultRecord"-Attribute auf Seite 133.
(2) Weitere Informationen dazu, wie Sie auf dieses Attribut zugreifen können, finden Sie im Abschnitt Erfassen von Fehlerinformationen auf Seite 134.
(3) Länge = 37.
(4) Von der Standard-Task ist die GSV-Zugänglichkeit der Sicherheitsobjektattribute die gleiche wie für Standardobjektattribute.

Zugreifen auf die „FaultRecord"-Attribute

Erstellen Sie eine benutzerdefinierte Struktur, um den Zugriff auf die Attribute „MajorFaultRecord" und „SafetyTaskFaultRecord" zu vereinfachen.

Tabelle 43 – Parameter für den Zugriff auf „FaultRecord"-Attribute

Name	Datentyp	Stil	Beschreibung
TimeLow	DINT	Dezimal	Die unteren 32 Bit des Werts für den Fehlerzeitstempel
TimeHigh	DINT	Dezimal	Die oberen 32 Bit des Werts für den Fehlerzeitstempel
Type	INT	Dezimal	Fehlertyp (Programm, E/A oder Sonstiges)
Code	INT	Dezimal	Eindeutiger Code für diesen Fehler (abhängig vom Fehlertyp)
Info	DINT[8]	Hexadezimal	Fehlerspezifische Informationen (abhängig vom Fehlertyp und -code)

Weitere Informationen zur Verwendung der GSV- und SSV-Befehle finden Sie im Kapitel zu den Eingabe-/Ausgabebefehlen in der Publikation 1756-RM003, Logix5000-Steuerungen – Allgemeine Befehle – Referenzhandbuch.

Erfassen von Fehlerinformationen

Die Attribute „SafetyStatus“ und „SafetyTaskFaultRecord“ können Informationen zu nicht korrigierbaren Fehlern erfassen. Verwenden Sie im Fehlerbearbeitungsprogramm der Steuerung einen GSV-Befehl, um die Fehlerinformationen zu erfassen und zu speichern. Der GSV-Befehl kann in einer Standard-Task in Verbindung mit einer Routine des Fehlerbearbeitungsprogramms der Steuerung verwendet werden, die den Fehler löscht und die weitere Ausführung der Standard-Tasks ermöglicht.

Statusanzeigen

Thema	Seite
Statusanzeigen der Steuerung	135
Statusanzeige der Steuerung	136

Statusanzeigen der Steuerung

Der Status der Primärsteuerung kann über vier Statusanzeigen abgelesen werden.

Tabelle 44 – Beschreibung der Statusanzeigen der Primärsteuerung

Anzeige	Status	Beschreibung
RUN	Aus	Es werden keine Benutzer-Tasks ausgeführt. Steuerung ist im PROGram-Modus.
	Grün	Steuerung ist im RUN-Modus.
FORCE	Aus	Keine Force-Zustände, Standard oder Sicherheit, sind auf der Steuerung aktiviert.
	Gelb	Standard- und/oder Sicherheits-Force-Zustände wurden aktiviert. **Gehen Sie beim Installieren (Hinzufügen) eines Force-Zustands vorsichtig vor. Nach dem Installieren eines Force-Zustands wird dieser sofort wirksam.**
	Gelb, blinkend	Für mindestens eine E/A-Adresse, Standard und/oder Sicherheit, wurde der Ein- oder Aus-Zustand geforct, wobei jedoch keine Force-Zustände aktiviert sind. **Gehen Sie beim Aktivieren von E/A-Force-Zuständen vorsichtig vor. Bei Aktivierung von E/A-Force-Zuständen werden auch alle bestehenden E/A-Force-Zustände wirksam.**
SD	Aus	Auf der Speicherkarte findet keine Aktivität statt.
	Grün, blinkend	Die Steuerung liest Daten von der Speicherkarte oder schreibt Daten darauf. Nehmen Sie die Speicherkarte nicht heraus, während die Steuerung Daten liest oder schreibt.
	Grün	
	Rot, blinkend	Die Speicherkarte verfügt über kein gültiges Dateisystem.
	Rot	Die Speicherkarte wird von der Steuerung nicht erkannt.
OK	Aus	Keine Stromversorgung.
	Grün	Die Steuerung arbeitet fehlerfrei.
	Rot, blinkend	• Nicht korrigierbarer Fehler oder korrigierbarer Fehler, der nicht in der Fehlerbehebung behandelt wurde. Alle Benutzer-Tasks, sowohl Standard als auch Sicherheit, werden beendet. • Wenn die Steuerung neu ist und noch nie verwendet wurde, ist ein Firmware-Upgrade erforderlich. Die Statusanzeige zeigt an, dass eine Firmwareinstallation erforderlich ist.
	Rot	• Die Steuerung führt eine Einschaltdiagnose durch. • Ein nicht korrigierbarer schwerwiegender Fehler ist aufgetreten und das Programm wurde vom Speicher gelöscht. • Die Ladung des Kondensators im Energiespeichermodul (ESM) wird beim Ausschalten entladen. • Die Steuerung ist eingeschaltet, aber nicht funktionsbereit. • Die Steuerung lädt ein Projekt in den nichtflüchtigen Speicher.

Der Sicherheitspartner verfügt über eine OK-Statusanzeige.

Tabelle 45 – 1756-L7SP – Statusanzeige

Anzeige	Status	Beschreibung
OK	Aus	Keine Stromversorgung.
	Grün	Der Sicherheitspartner arbeitet ohne Fehler.
	Rot	Die Steuerung schaltet sich ein oder ein nicht korrigierbarer Fehler ist aufgetreten.

Statusanzeige der Steuerung

Die Statusanzeige der Steuerung durchläuft Meldungen, die Informationen über die Firmwareversion, den Status des Energiespeichermoduls (ESM), den Projektstatus und schwerwiegende Fehler der Steuerung liefern.

Sicherheitsbezogene Statusmeldungen

Die Anzeige der Primärsteuerung kann die folgenden Meldungen anzeigen. Der Sicherheitspartner zeigt „L7SP“ an.

Tabelle 46 – Sicherheitsbezogene Statusanzeige

Meldung	Bedeutung
No Safety Signature	Sicherheits-Task wird im Run-Modus ohne Sicherheits-Task-Signatur ausgeführt.
Safety Partner Missing	Sicherheitspartner fehlt oder ist nicht verfügbar.
Hardware Incompatible	Hardware von Sicherheitspartner und Primärsteuerung sind nicht kompatibel.
Firmware Incompatible	Versionsstände der Hardware von Sicherheitspartner und Primärsteuerung sind nicht kompatibel.
No CST Master	Master für koordinierte Systemzeit (CST) wurde nicht gefunden.
Safety Task Inoperable	Sicherheitslogik ist ungültig. Dieser Fehler tritt auf, wenn z. B. keine Übereinstimmung zwischen der Primärsteuerung und dem Sicherheitspartner vorliegt, ein Timeout des Überwachungszeitraums erfolgt ist oder der Speicher fehlerhaft ist.
Safety Unlocked	Steuerung befindet sich im Run-Modus und verfügt über eine Sicherheitssignatur, ist jedoch nicht sicherheitsgesperrt.

Allgemeine Statusmeldungen

Die in Tabelle 47 beschriebenen Meldungen werden üblicherweise beim Ein- und Ausschalten und während des Betriebs der Steuerung angezeigt. Diese Meldungen informieren über den Status der Steuerung und des ESM.

Tabelle 47 – Allgemeine Statusanzeige

Meldung	Bedeutung
Keine Meldung	Die Steuerung ist ausgeschaltet oder ein nicht korrigierbarer schwerwiegender Fehler (MNRF) ist aufgetreten. Prüfen Sie die Statusleuchte „OK“, um zu ermitteln, ob die Steuerung eingeschaltet ist, und um den Zustand der Steuerung zu bestimmen.
TEST	Die Steuerung führt Einschalttests durch.
PASS	Die Einschalttests wurden erfolgreich abgeschlossen.
SAVE	Ein Projekt wird beim Abschalten auf die SD-Karte gespeichert. Weitere Statusinformationen können Sie an der Statusleuchte „SD“ ablesen (siehe Seite 135). Warten Sie, bis der Speichervorgang abgeschlossen ist, bevor Sie die SD-Karte ausbauen oder die Spannungsversorgung unterbrechen.
LOAD	Ein Projekt wird beim Einschalten von der SD-Karte auf die Steuerung geladen. Weitere Statusinformationen können Sie an der Statusleuchte „SD“ ablesen (siehe Seite 135). Warten Sie, bis der Ladevorgang abgeschlossen ist, bevor Sie die SD-Karte ausbauen, das ESM-Modul entfernen oder die Spannungsversorgung unterbrechen.
UPDT	Beim Einschalten wird ein Firmware-Upgrade von der SD-Karte ausgeführt. Weitere Statusinformationen können Sie an der Statusleuchte „SD“ ablesen (siehe Seite 135). Soll die Firmware beim Einschalten nicht aktualisiert werden, ändern Sie die Einstellung für die Eigenschaft „Load Image“ (Abbilddatei laden) der Steuerung.
CHRG (Aufladen)	Das kondensatorbasierte ESM wird geladen.
1756-L7*x*/*X*	Die Bestellnummer und Serie der Steuerung.
Rev *XX.xxx*	Die Haupt- und Nebenversion der Steuerungsfirmware.
No Project	In der Steuerung ist kein Projekt geladen. Verwenden Sie zum Laden eines Projekts in die Steuerung die Anwendung Logix Designer oder eine SD-Karte.
Project Name	Der Name des Projekts, das aktuell in der Steuerung geladen ist. Der angegebene Name basiert auf dem in der Anwendung Logix Designer festgelegten Projektnamen.
BUSY	Die E/A-Geräte, die der Steuerung zugewiesen sind, werden noch nicht vollständig mit Spannung versorgt. Warten Sie, bis der Einschaltvorgang und der Selbsttest der E/A-Geräte abgeschlossen sind.
Corrupt Certificate Received	Das der Firmware zugeordnete Sicherheitszertifikat ist fehlerhaft. Laden Sie unter http://www.rockwellautomation.com/support/ die Firmwareversion herunter, auf die Sie ein Upgrade durchführen möchten. Ersetzen Sie die zuvor installierte Firmwareversion durch die Version, die auf der Website des technischen Supports zur Verfügung gestellt wurde.
Corrupt Image Received	Die Firmwaredatei ist fehlerhaft. Laden Sie unter http://www.rockwellautomation.com/support/ die Firmwareversion herunter, auf die Sie ein Upgrade durchführen möchten. Ersetzen Sie die zuvor installierte Firmwareversion durch die Version, die auf der Website des technischen Supports zur Verfügung gestellt wurde.
ESM Not Present	Es ist kein ESM vorhanden und die Steuerung kann die Anwendung beim Ausschalten nicht speichern. Setzen Sie ein kompatibles ESM ein und unterbrechen Sie, sofern Sie ein kondensatorbasiertes ESM verwenden, die Spannungsversorgung erst, wenn das ESM geladen ist.
ESM Incompatible	Das ESM ist hinsichtlich der Speichergröße nicht mit der Steuerung kompatibel. Ersetzen Sie das inkompatible ESM durch ein kompatibles ESM.
ESM Hardware Failure	Es ist ein ESM-Fehler aufgetreten und die Steuerung kann das Programm im Falle einer Abschaltung nicht speichern. Ersetzen Sie das ESM, bevor Sie die Spannungsversorgung der Steuerung unterbrechen, damit das Steuerungsprogramm gespeichert werden kann.
ESM Energy Low	Das kondensatorbasierte ESM verfügt nicht über ausreichend Energie, um der Steuerung im Falle einer Abschaltung die Speicherung des Programms zu ermöglichen. Ersetzen Sie das ESM.
ESM Charging	Das kondensatorbasierte ESM wird geladen. Unterbrechen Sie die Spannungsversorgung erst, wenn der Ladevorgang abgeschlossen ist.
Flash in Progress	Ein von den Dienstprogrammen ControlFLASH oder AutoFlash eingeleitetes Firmware-Upgrade wird ausgeführt. Warten Sie, bis das Firmware-Upgrade abgeschlossen wurde, ohne den Vorgang zu unterbrechen.
Firmware Installation Required	Die Steuerung verwendet die Boot-Firmware (d. h. Version 1.*xxx*) und benötigt ein Firmware-Upgrade. Aktualisieren Sie die Steuerungsfirmware.
SD Card Locked	Es ist eine gesperrte SD-Karte installiert.

Fehlermeldungen

Wenn in der Steuerung ein Fehler auftritt, können in der Statusanzeige die folgenden Meldungen angezeigt werden.

Tabelle 48 – Fehlermeldungen(1)

Meldung	Bedeutung
Major Fault T*XX*:C*XX Meldung*	Es wurde ein schwerwiegender Fehler des Typs *XX* und mit dem Code *XX* erkannt. Wenn beispielsweise die Statusanzeige den schwerwiegenden Fehler „T04:C42 Invalid JMP Target“ anzeigt, ist ein JMP-Befehl so programmiert, dass zu einem ungültigen LBL-Befehl gewechselt wird.
I/O Fault Local:*X #XXXX*	An einem Modul im zentralen Chassis ist ein E/A-Fehler aufgetreten. Steckplatznummer und Fehlercode werden zusammen mit einer kurzen Beschreibung angegeben. So weist z. B. „I/O Fault Local:3 #0107 Connection Not Found“ darauf hin, dass eine Verbindung zum zentralen E/A-Modul in Steckplatz 3 nicht offen ist. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.
I/O Fault *ModuleName #XXXX*	An einem Modul in einem dezentralen Chassis ist ein E/A-Fehler aufgetreten. Der Name des fehlerhaften Moduls, wie er im E/A-Konfigurationsverzeichnis der Anwendung Logix Designer konfiguriert ist, wird mit dem Fehlercode und einer kurzen Beschreibung des Fehlers angezeigt. So weist z. B. „ I/O Fault My_Module #0107 Connection Not Found“ darauf hin, dass eine Verbindung zum Modul mit dem Namen „My_Module“ nicht offen ist. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.
I/O Fault *ModuleParent:X #XXXX*	An einem Modul in einem dezentralen Chassis ist ein E/A-Fehler aufgetreten. Es ist der Name des übergeordneten Moduls angegeben, da im E/A-Konfigurationsverzeichnis der Anwendung Logix Designer kein Modulname konfiguriert ist. Zusätzlich ist der Fehlercode mit einer kurzen Beschreibung des Fehlers angegeben. So weist z. B. „I/O Fault My_CNet:3 #0107 Connection Not Found“ darauf hin, dass eine Verbindung zu einem Modul in Steckplatz 3 des Chassis mit dem Kommunikationsmodul namens „My_CNet“ nicht offen ist. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.
X I/O Faults	Es liegen E/A-Fehler vor, wobei *X* die Anzahl der vorliegenden E/A-Fehler ist. Wenn mehrere E/A-Fehler vorliegen, gibt die Steuerung den zuerst gemeldeten Fehler an. Beim Beheben der einzelnen E/A-Fehler wird die angegebene Zahl der Fehler kleiner, während der nächste gemeldete Fehler von der E/A-Fehlermeldung angezeigt wird. Ergreifen Sie die erforderlichen Maßnahmen für den angegebenen Fehlertyp.

(1) Einzelheiten zu den einzelnen E/A-Fehlercodes finden Sie im Programmierhandbuch „Logix5000 Major, Minor, and I/O Fault Codes Programming Manual“, Publikation 1756-PM014.

Meldungen zu schwerwiegenden, korrigierbaren Fehlern

Auf schwerwiegende, korrigierbare Fehler wird durch die „Major Fault T*XX*:C*XX* in der Statusanzeige der Steuerung hingewiesen. In Tabelle 49 auf Seite 139 sind die speziellen Fehlertypen, Codes und die zugehörigen Meldungen aufgeführt, wie sie in der Statusanzeige erscheinen.

Ausführliche Beschreibungen und Vorschläge zur Behebung schwerwiegender, korrigierbarer Fehler finden Sie im Programmierhandbuch „Logix5000 Major, Minor, and I/O Fault Codes Programming Manual“, Publikation 1756-PM014.

Tabelle 49 – Statusmeldungen zu schwerwiegenden, korrigierbaren Fehlern

Type	Code	Meldung
1	1	Run Mode Powerup
1	60	Non-recoverable
1	61	Non-recoverable – Diagnostics Saved
1	62	Non-recoverable – Program Saved
3	16	I/O Connection Failure
3	20	Chassis Failure
3	21	
3	23	Connection Failure
4	16	Unknown Instruction
4	20	Invalid Array Subscript
4	21	Control Structure LEN or POS < 0
4	31	Invalid JSR Parameter
4	34	Timer Failure
4	42	Invalid JMP Target
4	82	SFC Jump Back Failure
4	83	Value Out of Range
4	84	Stack Overflow
4	89	Invalid Target Step
4	90	Invalid Instruction
4	91	Invalid Context
4	92	Invalid Action
4	990	Benutzerdefiniert
4	991	
4	992	
4	993	
4	994	
4	995	
4	996	
4	997	
4	998	
4	999	
6	1	Task Watchdog Expired
7	40	Save Failure
7	41	Bad Restore Type
7	42	Bad Restore Revision
7	43	Bad Restore Checksum
8	1	Keyswitch Change Ignored
11	1	Positive Overtravel Limit Exceeded
11	2	Negative Overtravel Limit Exceeded
11	3	Position Error Tolerance Exceeded
11	4	Encoder Channel Connection Fault
11	5	Encoder Noise Event Detected
11	6	SERCOS Drive Fault
11	7	Synchronous Connection Fault
11	8	Servo Module Fault
11	9	Asynchronous Connection Fault
11	10	Motor Fault
11	11	Motor Thermal Fault
11	12	Drive Thermal Fault
11	13	SERCOS Communications Fault
11	14	Inactive Drive Enable Input Detected
11	15	Drive Phase Loss Detected
11	16	Drive Guard Fault
11	32	Motion Task Overlap Fault
11	33	CST Reference Loss Detected
18	1	CIP Motion Initialization Fault
18	2	CIP Motion Initialization Fault Mfg
18	3	CIP Motion Axis Fault
18	4	CIP Motion Axis Fault Mfg
18	5	CIP Motion Fault
18	6	CIP Module Fault
18	7	Motion Group Fault
18	8	CIP Motion Configuration Fault
18	9	CIP Motion APR Fault
18	10	CIP Motion APR Fault Mfg
18	128	CIP Motion Guard Fault

E/A-Fehlercodes

E/A-Fehler, die von der Steuerung angezeigt werden, erscheinen in der Statusanzeige in einem dieser Formate:

- I/O Fault Local:*X #XXXX*
- I/O Fault *ModuleName #XXXX*
- I/O Fault *ModuleParent*:*X #XXXX*

Der erste Teil des Formats gibt die Position des fehlerhaften Moduls an. Wie die Position angegeben wird, hängt von Ihrer E/A-Konfiguration und den in der Anwendung „Logix Designer“ angegebenen Moduleigenschaften ab.

Der letzte Teil des Formats, „#XXXX“, kann für die Diagnose des E/A-Fehlertyps und der möglichen Gegenmaßnahmen verwendet werden. Einzelheiten zu den einzelnen E/A-Fehlercodes finden Sie im Programmierhandbuch „Logix5000 Major, Minor, and I/O Fault Codes Programming Manual“, Publikation 1756-PM014.

Tabelle 50 – E/A-Fehlermeldungen

Code	Meldung
#0001	Connection Failure
#0002	Insufficient Resource
#0003	Invalid Value
#0004	IOI Syntax
#0005	Destination Unknown
#0006	Partial Data Transferred
#0007	Connection Lost
#0008	Service Unsupported
#0009	Invalid Attribute Value
#000A	Attribute List Error
#000B	State Already Exists
#000C	Object Mode Conflict
#000D	Object Already Exists
#000E	Attribute Not Setable
#000F	Permission Denied
#0010	Device State Conflict
#0011	Reply Too Large
#0012	Fragment Primitive
#0013	Insufficient Command Data
#0014	Attribute Not Supported
#0015	Data Too Large
#0100	Connection In Use
#0103	Transport Not Supported
#0106	Ownership Conflict
#0107	Connection Not Found
#0108	Invalid Connection Type
#0109	Invalid Connection Size
#0110	Module Not Configured
#0111	RPI Out of Range
#0113	Out of Connections
#0114	Wrong Module

Code	Meldung
#0115	Wrong Device Type
#0116	Wrong Revision
#0117	Invalid Connection Point
#0118	Invalid Configuration Format
#0119	Module Not Owned
#011A	Out of Connection Resources
#0203	Connection Timeout
#0204	Unconnected Message Timeout
#0205	Invalid Parameter
#0206	Message Too Large
#0301	No Buffer Memory
#0302	Bandwidth Not Available
#0303	No Bridge Available
#0304	ControlNet Schedule Error
#0305	Signature Mismatch
#0306	CCM Not Available
#0311	Invalid Port
#0312	Invalid Link Address
#0315	Invalid Segment Type
#0317	Connection Not Scheduled
#0318	Invalid Link Address
#0319	No Secondary Resources Available
#031E	No Available Resources
#031F	No Available Resources
#0800	Network Link Offline
#0801	Incompatible Multicast RPI
#0802	Invld Safety Conn Size
#0803	Invld Safety Conn Format
#0804	Invld Time Correct Conn Format
#0805	Invld Ping Intrvl EPI Multiplier
#0806	Time Coord Msg Min Multiplier

E/A-Fehlermeldungen (Fortsetzung)

Code	Meldung
#0807	Time Expectation Multiplier
#0808	Timeout-Multiplikator
#0809	Invld Max Consumer Number
#080A	Invld CPCRC
#080B	Time Correction Conn ID Invld
#080C	Safety Cfg Signature Mismatch
#080D	Safety Netwk Num Not Set OutOfBx
#080E	Safety Netwk Number Mismatch
#080F	Cfg Operation Not Allowed
#0814	Data Type Mismatch
#FD01	Bad Backplane EEPROM
#FD02	No Error Code
#FD03	Missing Required Connection
#FD04	No CST Master
#FD05	Axis or GRP Not Assigned
#FD06	SERCOS Transition Fault
#FD07	SERCOS Init Ring Fault
#FD08	SERCOS Comm Fault
#FD09	SERCOS Init Node Fault
#FD0A	Axis Attribute Reject
#FD1F	Safety Data Fault
#FD20	No Safety Task Running
#FD21	Invld Safety Conn Parameter
#FE01	Invalid Connection Type
#FE02	Invalid Update Rate
#FE03	Invalid Input Connection
#FE04	Invalid Input Data Pointer
#FE05	Invalid Input Data Size
#FE06	Invalid Input Force Pointer
#FE07	Invalid Output Connection

Code	Meldung
#FE08	Invalid Output Data Pointer
#FE09	Invalid Output Data Size
#FE0A	Invalid Output Force Pointer
#FE0B	Invalid Symbol String
#FE0C	Invalid Scheduled P/C Instance
#FE0D	Invalid Symbol Instance
#FE0E	Module Firmware Updating
#FE0F	Invalid Firmware File Revision
#FE10	Firmware File Not Found
#FE11	Firmware File Invalid
#FE12	Automatic Firmware Update Failed
#FE13	Update Failed – Active Connection
#FE14	Searching Firmware File
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
#FE22	Invalid Connection Type
#FE23	Invalid Unicast Allowed
#FF00	No Connection Instance
#FF01	Path Too Long
#FF04	Invalid State
#FF08	Invalid Path
#FF0B	Invalid Config
#FF0E	No Connection Allowed
—	

Notizen:

Wechsel des Steuerungstyps

Thema	Seite
Wechsel von Standard- zu Sicherheitssteuerung	143
Wechsel von Sicherheits- zu Standardsteuerung	144
Wechsel von Sicherheitssteuerungstypen	144
Weitere Informationen	145

Da Sicherheitssteuerungen besonderen Anforderungen unterliegen und bestimmte Standardfunktionen nicht unterstützen, müssen Sie das Verhalten des Systems verstehen, wenn Sie in Ihrem Steuerungsprojekt von einer Standard- zu einer Sicherheitssteuerung oder von einer Sicherheits- zu einer Standardsteuerung wechseln. Der Wechsel des Steuerungstyps wirkt sich auf Folgendes aus:

- Unterstützte Leistungsmerkmale
- Physische Konfiguration des Projekts (Sicherheitspartner und Sicherheits-E/A)
- Steuerungseigenschaften
- Projektkomponenten (z. B. Tasks, Programme, Routinen und Tags)
- Sicherheitsrelevante Add-On-Befehle

WICHTIG GuardLogix-Steuerungen der Serie 5560 und Compact GuardLogix-Steuerungen der Serie 1768 werden in Studio 5000, Version 21 oder höher, nicht unterstützt.

Wechsel von Standard- zu Sicherheitssteuerung

Um erfolgreich von einer Standardsteuerung zu einer Sicherheitssteuerung zu wechseln, muss für den Sicherheitspartner der Chassissteckplatz rechts neben der Sicherheitsprimärsteuerung frei sein.

Nach der Bestätigung des Wechsels von einem Projekt mit Standardsteuerung zu einem Projekt mit Sicherheitssteuerung werden Sicherheitskomponenten erstellt, damit die Mindestanforderungen an eine Sicherheitssteuerung erfüllt werden:

- Die Sicherheits-Task wird nur erstellt, wenn die maximal herunterladbare Anzahl von Tasks noch nicht erreicht ist. Die Sicherheits-Task wird mit ihren Standardwerten initialisiert.
- Sicherheitskomponenten werden erstellt (Sicherheits-Task, Sicherheitsprogramm usw.).
- Eine zeitbasierte Sicherheitsnetzwerknummer (SNN) wird für das lokale Chassis generiert.

- Alle nicht von der Sicherheitssteuerung unterstützten Standardsteuerungsfunktionen, wie z. B. Redundanz, stehen im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) nicht mehr zur Verfügung (sofern dies zuvor der Fall war).

Wechsel von Sicherheits- zu Standardsteuerung

Nach der Bestätigung eines Wechsels von einem Projekt mit Sicherheitssteuerung zu einem Projekt mit Standardsteuerung werden einige Komponenten geändert und andere gelöscht, wie nachfolgend beschrieben:

- Der Sicherheitspartner wird aus dem E/A-Chassis entfernt.
- Sicherheits-E/A-Geräte und ihre Tags werden gelöscht.
- Sicherheits-Task, Sicherheitsprogramme und Sicherheitsroutinen werden in Standard-Tasks, Standardprogramme und Standardroutinen geändert.
- Alle Sicherheits-Tags, ausgenommen konsumierte Sicherheits-Tags, werden in Standard-Tags geändert. Konsumierte Sicherheits-Tags werden gelöscht.
- Sicherheits-Tag-Zuordnungen werden gelöscht.
- Die Sicherheitsnetzwerknummer (SNN) wird gelöscht.
- Sicherheitssperrungs- und Sicherheitsentsperrungs-Kennwörter werden gelöscht.
- Wenn die Standardsteuerung Funktionen unterstützt, die für die Sicherheitssteuerung nicht zur Verfügung standen, werden diese neuen Merkmale im Dialogfeld „Controller Properties“ (Steuerungseigenschaften) angezeigt.

  HINWEIS Peer-Sicherheitssteuerungen werden nicht gelöscht, selbst wenn sie keine Verbindungen mehr haben.

- Befehle können weiterhin auf Module verweisen, die bereits gelöscht wurden. In diesem Fall werden Verifizierungsfehler generiert.
- Konsumierte Tags werden beim Löschen des produzierenden Moduls ebenfalls gelöscht.
- Aufgrund der oben durchgeführten Systemänderungen werden sicherheitsspezifische Befehle und Sicherheits-E/A-Tags nicht verifiziert.

Enthält das Sicherheitssteuerungsprojekt Sicherheits-Add-On-Befehle, müssen Sie diese vor dem Wechsel des Steuerungstyps aus dem Projekt entfernen oder deren Klasse wieder in „Standard“ ändern.

Wechsel von Sicherheitssteuerungstypen

WICHTIG Compact GuardLogix-Steuerungen der Serie 1768 und GuardLogix-Steuerungen der Serie 5560 werden in der Anwendung Logix Designer, Version 21, nicht unterstützt.

Wenn Sie von einem Sicherheitssteuerungstyp zu einem anderen wechseln, bleibt die Klasse der Tags, Routinen und Programme unverändert. Alle E/A-Geräte, die nicht mehr mit der Zielsteuerung kompatibel sind, werden gelöscht.

Die Darstellung des Sicherheitspartners wird so aktualisiert, dass sie für die Zielsteuerung geeignet ist:

- Der Sicherheitspartner wird in Steckplatz *x* (primärer Steckplatz + 1) erstellt, wenn Sie von einer Compact GuardLogix-Steuerung der Serie1768 zu einer GuardLogix-Steuerung der Serie 5570 wechseln.
- Beim Wechsel zu einer Compact GuardLogix-Steuerung der Serie 1768 wird der Sicherheitspartner entfernt, da dieser sich innerhalb der Compact GuardLogix-Steuerung befindet.

HINWEIS Eine GuardLogix-Steuerung der Serie 5570 unterstützt 100 Sicherheitsprogramme in der Sicherheits-Task, während eine Compact GuardLogix-Steuerung der Serie 1768 32 Sicherheitsprogramme unterstützt.

Fließkommabefehle, wie z. B. FAL, FLL, FSC, SIZE, CMP, SWPB und CPT, werden in GuardLogix-Steuerungen der Serie 5570 unterstützt, jedoch nicht in GuardLogix-Steuerungen der Serie 5560 und Compact GuardLogix-Steuerungen der Serie 1768. Wenn Ihr Sicherheitsprogramm diese Befehle enthält, werden beim Wechsel von einer GuardLogix-Steuerung der Serie 5570 zu einer GuardLogix-Steuerung der Serie 5560 oder Compact GuardLogix-Steuerung der Serie 1768 Verifizierungsfehler generiert.

Weitere Informationen

Weitere Informationen zu Add-On-Befehlen finden Sie in der Publikation 1756-PM010, Logix5000 Controllers Add-On Instructions Programming Manual.

Notizen:

Ziffern

1756-Axx 29
1756-CN2 62
1756-CN2R 62
1756-CN2RXT 62
1756-CNB 62
1756-CNBR 62
1756-DNB 64, 66, 111
1756-EN2F 57
1756-EN2T 57
1756-EN2TR 57
1756-EN2TRXT 57
1756-EN2TXT 57
1756-EN3TR 57
1756-ENBT 57
1756-ESMCAP 28, 39, 41, 122, 124
1756-ESMCAPXT 28, 39, 41, 122, 124
1756-ESMNRM 28, 40, 41, 122, 124
1756-ESMNRMXT 28, 41, 122, 124
1756-ESMNSE 28, 40, 41, 122, 124
1756-ESMNSEXT 28, 41, 122, 124
1756-EWEB 57
1756-PA72 29
1756-PA75 29
1756-PAXT 29
1756-PB72 29
1756-PB75 29
1756-PBXT 29
1756-SPESMCAP 28, 39
1756-SPESMNRM 28, 41, 122
1756-SPESMNRMXT 28, 41, 122
1756-SPESMNSE 28, 40, 41, 122
1756-SPESMNSEXT 28, 39, 41, 122
1768 Compact GuardLogix-Steuerung 145
1784-SD1 28
1784-SD2 28

A

Abtastzeiten
zurücksetzen 110
Add-On-Befehle 23, 144
Adresse
Kinetix-Sicherheits-E/A-Gerät 78
Alias-Tags 95
allgemeine Statusmeldungen 137
Angefordertes Paketintervall (RPI) 99
Definition 13
konsumierte Tags 95
konsumiertes Tag 103
produzierte Tag-Daten 95
Sicherheits-E/A 72
Anwenderspeicher 20
anzeigen
Sicherheitsstatus 113
Attribute
Sicherheitsobjekt 132
Ausfallwahrscheinlichkeit bei Anforderung (PFD)
Definition 13
Ausfallwahrscheinlichkeit pro Stunde (PFH)
Definition 13
austauschen
Configure Always (Immer konfigurieren) aktiviert 86
Configure Only (Nur konfigurieren) … aktiviert 82
Guard I/O-Modul 81-90
AutoFlash
Firmware-Update 37
automatische Firmware-Updates 124
azyklische Verbindungen 63

B

Basis-Tags 95
BAT-Anzeige 125
Batterie
Fehler 125
Bearbeitung 109
beobachtete maximale Netzwerkverzögerung 72
zurücksetzen 103
Betriebsart 38

C

Chassis 21
Bestellnummer 29
CIP Safety 13, 51, 87
CIP Safety-E/A
Hinzufügen 67
Konfigurationssignatur 75
Netzknotenadresse 67
Statusdaten 79
Überwachen des Status 79
Verwaltungsberechtigung zurücksetzen 76
Compact GuardLogix-Steuerung 145
Configure Always (immer konfigurieren) 86
Optionsfeld 49
CONNECTION_STATUS 99, 127
ConnectionFaulted-Bit 127
ControlFLASH, Software 36, 113, 121, 124
ControlNet
azyklisch 63
Beispiel 63
Kommunikationsmodule 22
Modul 62, 111
Software 62
Treiber konfigurieren 112
Überblick 62
Verbindungen 63, 112
zyklisch 63

D

Datentypen
CONNECTION_STATUS 99
DeviceNet
Kommunikation 64
Modul 111
Software 65
Treiber konfigurieren 112
Verbindungen 66, 112
Diagnoseabdeckung 13
Dialogfeld „New Controller“ (Neue Steuerung) 43
DNT-Datei 89, 90

E

E/A
Anzeige 126
Fehlercodes 140
Modulaustausch 48
einfügen
Sicherheitsnetzwerknummer 56
Einschränkungen
Programmierung 110
Software 110
wenn eine Sicherheitssignatur besteht 109
wenn sicherheitsgesperrt 106
Zuordnung von Sicherheits-Tags 104
Einschränkungen bei der Programmierung 110
elektronische Codierung 124
elektrostatische Entladung 28
Energiespeichermodul 28
1756-ESMCAP 28
Aufladen 30, 42
Definition 13
deinstallieren 39
einbauen, installieren 41
Haltezeit 124
nichtflüchtiger Speicher 122
Erstellen eines Projekts 43
Erstellen eines Tags 101
Erweiterte Verbindungsreaktionszeit der Verbindung 73
ESM
Siehe „Energiespeichermodul“
EtherNet/IP
Beispiel 59
Gerät 111
Kommunikationsmodule 22
Module 57
Modulfunktion 58
Netzwerkparameter 61
Sicherheits-E/A-Gerät 60
Standard-E/A-Module 61
Treiber konfigurieren 112
Überblick 57
Verbindungen 58, 111
Verbindungsverwendung 58
Externer Zugriff 94, 98
extreme Umgebungsbedingungen
Chassis 29
Netzteil 29
Steuerung 12
Systemkomponenten 12

F

Fehler
korrigierbar 129, 139
löschen 129
Meldungen 138, 139
nicht korrigierbarer Fehler, Sicherheit 128, 129
nicht korrigierbarer Fehler, Steuerung 129
Routinen 131-133
Fehlercodes
E/A-Meldungen 140
schwerwiegende Sicherheitsfehler 130
Statusanzeige 130
Firmware Supervisor 124
Firmware-Upgrade-Kit 113, 124
Firmwareversion
Fehlende Übereinstimmung 114, 116, 118
Übereinstimmung 113
Update 36, 37
Verwaltung 124
Forcieren 109

G

Gateway 61
Gehäuse 25
Guard I/O-Modul
Austausch 87-90
GuardLogix-Steuerungen
Unterschiede 11

H

Haltezeit
Energiespeichermodul 124
Herunterladen
Auswirkungen auf die Sicherheits-Task-Signatur 114
Auswirkungen der Firmware-Versionsübereinstimmung 113
Auswirkungen der Sicherheitssperre 114
Auswirkungen der Steuerungsübereinstimmung 113
Auswirkungen des Sicherheitsstatus 113
Prozess 115-116
HMI-Geräte 18
Hochladen
Auswirkungen auf die Sicherheits-Task-Signatur 114
Auswirkungen der Sicherheitssperre 114
Auswirkungen der Steuerungsübereinstimmung 113
Prozess 116

I

IP-Adresse 61, 67

K

Kennwort
festlegen 47
Gültige Zeichen 47
Kinetix 5500-Servoantrieb 60
Klasse 97
Kommunikation 22
ControlNet-Netzwerk 62
DeviceNet-Netzwerk 64
EtherNet/IP-Netzwerk 57
Module 22
Konfigurationssignatur
Definition 75
Komponenten 75
kopieren 75
Konfigurationsverwalter 76
identifizieren 76
Zurücksetzen 76, 80
Konsumieren von Tag-Daten 102
konsumiertes Tag 95, 98
koordinierte Systemzeit 116, 136
kopieren
Sicherheitsnetzwerknummer 56
Sicherheits-Task-Signatur 109
korrigierbarer Fehler 129, 139
löschen 129

L

Laden eines Projekts 121
On Corrupt Memory (Bei beschädigtem Speicher) 121
On Power Up (Beim Einschalten) 121
User Initiated (Vom Anwender initiiert) 121
Listen-only-Verbindung 76
Logix-XT-Systemkomponenten
Siehe „Extreme Umgebungsbedingungen“.
löschen
Fehler 129
Programm 123
Sicherheits-Task-Signatur 109

M

MajorFaultRecord 133
Meldung
Statusanzeige 137
Meldungen
allgemeiner Status 137
Fehler 138
Sicherheitsstatus 136
Modul
ControlNet 22
DeviceNet 22
Eigenschaften
Registerkarte „Verbindung“ 76
EtherNet/IP 22
Statusanzeige 79
Modul zurücksetzen 80
Module
EtherNet/IP 57
Modus
Betrieb 38
Multicast 13

N

Network Address Translation (NAT)
Definition 13
Festlegen der IP-Adresse 69
Unterstützte Leistungsmerkmale 23
Netzknotenadresse 67
Netzteil
Bestellnummer 21, 29
Netzwerkstatus
Anzeige 79, 83, 85, 89
Netzwerkverzögerungs-Multiplikator 74, 103
nicht korrigierbarer Sicherheitsfehler 128, 129
Neustarten der Sicherheits-Task 129
nicht korrigierbarer Steuerungsfehler 129
nichtflüchtiger Speicher 119-124
Registerkarte 120

O

online schalten 117
Faktoren 112
Online-Leiste 125

P

Peer-Sicherheitssteuerung
Gemeinsame Datennutzung 99
Konfiguration 50
Position 99
SNN 99
Performance Level (Leistungsstufe) 13, 17
Primärsteuerung
Anwenderspeicher 20
Beschreibung 20
Hardware-Überblick 20
Modi 20
Produzieren und Konsumieren von Tags 58, 62, 98
Produziertes Tag 95, 98
Programmbereichs-Tags 97
Programmfehlerroutine 131
Programmierung 109
Programm-Modus 38

R

RAM-Kapazität 20
Reaktionszeit 93
Reaktionszeitgrenze
CIP Safety-E/A 71
Reaktionszeitgrenze der Verbindung 71, 103
Registerkarte „Geringfügige Fehler“ 130
Registerkarte „Schwerwiegende Fehler“ 130

Registerkarte „Sicherheit“ 107, 108, 128
Einsehen des Sicherheitsstatus 113, 128
Erstellen einer Sicherheits-Task-Signatur 108
Konfigurationssignatur 75
Modulaustausch 81
sicherheitsgesperrte Steuerung 107
Sicherheitssperre 107
Sperre deaktivieren 107
Verbindungsdaten 71
Remote-Modus 38, 39
RPI
siehe Requested Packet Interval/ angefordertes Paketintervall
RunMode-Bit 127
Run-Modus 38
Run-Modus-Schutz 108, 109

S

SafetyTaskFaultRecord 133
Schlüsselschalter 20, 38
Schutz der Sicherheitsanwendung 106-109
Sicherheit 108
Sicherheitssperre 106
Sicherheits-Task-Signatur 108
schwerwiegende Sicherheitsfehler 130
schwerwiegende, korrigierbare Fehler 139
Meldungen 139
SD-Karte 28
ausbauen 31
einbauen, installieren 32
Siehe „SD-Karte“.
SD-Karte (Secure Digital)
Siehe auch „Speicherkarte“.
Seriennummer 113
Sicherer Zustand 17
Sicherheitsentsperrung
Steuerung 107
Symbol 107
Sicherheitsnetzwerknummer
Ändern der E/A-SNN 55
Ändern der Steuerungs-SNN 54
Änderung 54
anzeigen 45
automatische Zuweisung 53
Beschreibung 17
Definition 13
einfügen 56
Fehlende Übereinstimmung 88
festlegen 71
kopieren 56
Kopieren und Einfügen 56
manuell 53
manuelle Zuweisung 53
Verwalten 51
zeitbasiert 52
Zuweisung 51
Sicherheitsobjekt
Attribute 132
Sicherheitspartner
Beschreibung 21
Konfiguration 21
Status 128
Sicherheitsprogramme 93
Sicherheitsprojekte
Funktionen 23
Sicherheitsroutine 94
Verwenden von Standarddaten 104
Sicherheitssperre 106
Auswirkungen auf das Herunterladen 114
Auswirkungen auf das Hochladen 114
Kennwort 107
Steuerung 107
Symbol 107
Sicherheitsstatus
anzeigen 113, 125, 128
Auswirkungen auf das Herunterladen 113
Einschränkungen bei der Programmierung 110
Schaltfläche 108, 126
Sicherheits-Task-Signatur 108
Sicherheits-Tags
Beschreibung 94
erstellen 94
gültige Datentypen 96
Sicherheits-Programmbereich 97
Steuerungsbereich 97
Zuordnen (Mapping) 104-106
Sicherheits-Task 92
Ausführung 93
Priorität 92
Überwachungszeitraum 92
Sicherheits-Task-Signatur 98
anzeigen 125
Auswirkungen auf das Herunterladen 114
Auswirkungen auf das Hochladen 114
Beschreibung 18
eingeschränkte Operationen 109
Einschränkungen 110
generieren 108
kopieren 109
löschen 109
Speichern eines Projekts 120
Sicherheits-Task-Zeitspanne 72, 93, 99
Signatur im Run-Modus schützen 47
Software
ControlNet-Netzwerk 62
DeviceNet-Netzwerke 65
Einschränkungen 110
USB 33
Software RSLinx Classic
Version 22
Software RSLogix 5000
Einschränkungen 110
Software RSNetWorx for DeviceNet
Modul austauschen 87
Speicher
Kapazität 20
Speicherkarte 119, 121, 124
Ausbau 31
Installation 31
Speichern des Programms
nichtflüchtiger Speicher 122
Speichern eines Projekts 120
Sperre
Siehe „Sicherheitssperre“.
Sperre der Steuerung deaktivieren 107
Standarddaten in einer Sicherheitsroutine 104

Status
Anzeige 136-141
Fehlermeldungen 138
Meldungen 136
Meldungen, Anzeige 137
Sicherheitspartner 128
Statusanzeigen 135-136
E/A-Module 79
Status-Flags 127
Steckplatznummer 44
Steuerung
Aufzeichnen, Protokollieren
Sicherheitssperre aktivieren, deaktivieren 107
Sicherheits-Task-Signatur 109
Betriebsart 38, 39
Eigenschaften 45
extreme Umgebungsbedingungen 12
Fehlerbehebungsprogramm 131
Installation 29
keine Übereinstimmung zwischen Seriennummern 115, 118
Konfiguration 43
Modus 38
Seriennummer 113
Typ wechseln 143-145
Übereinstimmung 113
unterschiedliche Eigenschaften 11
Steuerungen wechseln 144
Steuerungs- und Informationsprotokoll
Definition 13
Steuerungsbereichs-Tags 96
Subnetz-Maske 61
Systemwert abrufen (GSV)
Definition 13
Verwendung 132
Zugänglichkeit 132
Systemwert einstellen (SSV)
Verwendung 132
Zugänglichkeit 132

T

Tag mit konstantem Wert 98
Tags
Alias 95
Basis 95
Bereich 96
Datentyp 95
Externer Zugriff 94, 98
Klasse 97
konstanter Wert 98
konsumiert 95, 98
Name 77
produziert 95, 98
produzierte/konsumierte Sicherheitsdaten 96, 97
Programmbereich 97
Sicherheits-E/A 96, 97
Siehe auch Sicherheits-Tags.
Steuerungsbereich 96
Typ 95
Überblick 94
Terminologie 13
Timeout-Multiplikator 73, 103
Treiber
ControlNet 112
DeviceNet 112
EtherNet/IP 112
USB 34

U

Übereinstimmung zwischen Projekt und Steuerung 113
überwachen
Status 79
Verbindungen 126
Überwachungszeitraum 92
Umgebung 25
Unicast 13
Verbindungen 98, 101
Update
Firmware 36, 37
USB
Anschluss 33
erforderliche Software 33
Kabel 33, 111
Treiber 34
Typ 33
Verbindung 34
UV-Strahlung 27

V

Verbindung
azyklisch 63
ControlNet-Netzwerk 63
EtherNet/IP-Netzwerk 58
Status 127
überwachen 126
USB 34
zyklisch 63
Verifizierungsfehler
Wechsel des Steuerungstyps 145
Verwaltungsberechtigung
Konfiguration 76
Zurücksetzen 76

W

WallClockTime (Uhrzeit) 122, 124
Energiespeichermodul 124
Objekt 42
Warnsymbol 126
Werkseinstellungen, -zustand 83
Modul zurücksetzen 80

X

XT
Siehe „Extreme Umgebungsbedingungen“.

Z

Zeitsynchronisierung 49, 116
Ziehen und Stecken unter Spannung 26
Siehe „Ziehen und Stecken unter Spannung“
Zulassung für explosionsgefährdete Standorte
Europa 27
Nordamerika 26
zurücksetzen
Modul 80
Verwaltungsberechtigung 76, 80
zyklische Verbindungen 63

Kundendienst von Rockwell Automation

Rockwell Automation bietet Ihnen über das Internet technische Informationen zur Unterstützung bei der Verwendung seiner Produkte. Unter http://www.rockwellautomation.com/Support finden Sie technische Informationen und Anwendungshinweise, Beispielcode sowie Links zu Software-Servicepaketen. Besuchen Sie unser Supportcenter unter https://rockwellautomation.custhelp.com/. Dort finden Sie Softwareupdates, Support-Chats und -Foren, technische Informationen und Antworten auf häufig gestellte Fragen. Darüber hinaus können Sie sich unter dieser Adresse anmelden, um über Produktupdates benachrichtigt zu werden.

Darüber hinaus stehen Ihnen verschiedene Support-Programme zur Installation, Konfiguration und Fehlerbehebung zur Verfügung. Wenn Sie weitere Informationen wünschen, wenden Sie sich an Ihren Distributor oder Vertreter von Rockwell Automation oder besuchen Sie uns unter http://www.rockwellautomation.com/services/online-phone.

Unterstützung bei der Installation

Falls innerhalb der ersten 24 Stunden nach der Installation ein Problem auftritt, lesen Sie bitte die Informationen in diesem Handbuch. Beim Kundendienst erhalten Sie Unterstützung beim Einrichten und Inbetriebnehmen IhresProdukts.

USA oder Kanada	+1 440 646 3434
Außerhalb der USA oder Kanada	Verwenden Sie den Worldwide Locator unter http://www.rockwellautomation.com/rockwellautomation/support/overview.page oder wenden Sie sich an die für Sie zuständige Vertretung von Rockwell Automation.

Rückgabeverfahren bei neuen Produkten

Rockwell Automation testet alle seine Produkte, um ab Werk die ordnungsgemäße Funktion gewährleisten zu können. Sollte das Produkt dennoch nicht ordnungsgemäß funktionieren und zurückgegeben werden müssen, gehen Sie wie folgt vor.

USA	Wenden Sie sich an Ihren Distributor. Teilen Sie ihm die Kundendienst-Bearbeitungsnummer mit, die Sie über die oben genannte Telefonnummer erhalten, damit das Rückgabeverfahren abgewickelt werden kann.
Außerhalb der USA	Bitte wenden Sie sich bei Fragen zum Rückgabeverfahren an die für Sie zuständige Vertretung von Rockwell Automation.

Feedback zur Dokumentation

Dank Ihrer Kommentare können wir Ihre Dokumentationsanforderungen besser erfüllen. Ihre Kommentare helfen uns, die Dokumentation entsprechend Ihren Anforderungen zu gestalten. Wenn Sie Vorschläge zur Verbesserung dieses Dokuments haben, füllen Sie bitte das entsprechende Formular, Publikation RA-DU002, abrufbar unter http://www.rockwellautomation.com/literature/, aus.

Rockwell Automation bietet auf der Website auch aktuelle Umweltinformationen zu den Produkten unter http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page.

www.rockwellautomation.com

Hauptverwaltung für Antriebs-, Steuerungs- und Informationslösungen

Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Naher Osten/Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asien/Australien/Pazifikraum: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, China, Tel: +852 2887 4788, Fax: +852 2508 1846

Deutschland: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
Schweiz: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
Österreich: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Publikation 1756-UM022C-DE-P – Mai 2015

© 2015 Rockwell Automation, Inc. Alle Rechte vorbehalten. Printed in the USA.